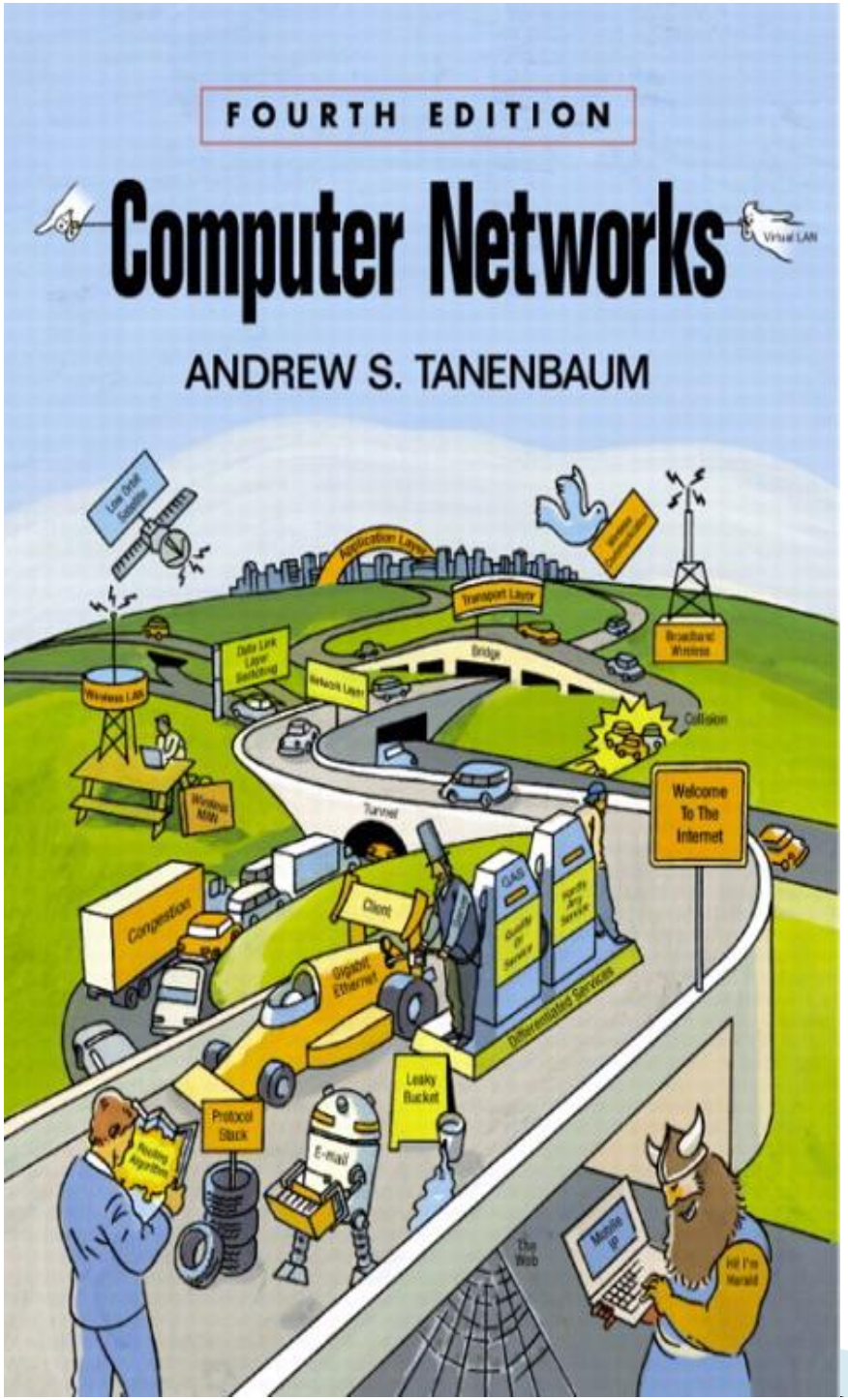
به نام خدا

شبکه های کامپیوتری

مدرس: مهندس ملیحه امینی



منابع

1)Computer Networks, By A.Tanenbaum

2)Data and Computer Communications, By W.stallings

3) Network Tutorial, By Steve Steinke

4) TCP/IP Fundations, By Sybex Author Assoc

4)MCSE Series, Essential Network

5)MCSE Series, TCP/IP

ارزشیابی

1)آزمون میان ترم 6 نمره
2) آزمون پایان ترم 12 نمره
3) حضور -کوئیز 2 نمره
4) ارائه 1+ نمره

فصل اول: مفاهیم شبکه‌های کامپیوتری

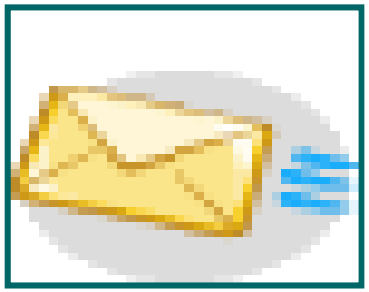
هدفهای آموزشی :

- مفهوم شبکه و کاربردهای آن
- سخت‌افزار شبکه
- انواع سوئیچینگ
- طراحی شبکه و اصول لایه‌بندی
- مدل هفت‌لایه‌ای OSI از سازمان استاندارد جهانی
- مدل چهارلایه‌ای TCP/IP


شبکه‌های کامپیوتری مجموعه‌ای از کامپیوترهای مستقل است که به نحوی با یکدیگر اطلاعات و داده مبادله می‌نمایند.
استقلال کامپیوترها
کارکردن هر ماشین به تنهایی در صورت نبودن در شبکه
تبادل داده
ردوبدل‌نمودن داده بدون توجه به نوع کانال انتقال

اهداف و مزایای شبکه‌های کامپیوتری

1. سهولت انتقال داده
2. اشتراک منابع
3. صرفه جویی در هزینه‌ها
4. افزایش قابلیت اطمینان
5. افزایش سرعت
6. جنبه سرگرمی
7. ایجاد ارتباط بین کاربران



خدمات معمول در شبکه

دسترسی به بانکهای اطلاعاتی راه دور

پست الکترونیکی

خدمات انتقال فایل

ورود به سیستم از راه دور

گروههای خبری

جستجوی اطلاعات مورد نیاز

تبلیغات

تجارت الکترونیکی

بانکداری الکترونیکی

سرگرمی و محاوره

مجلات و روزنامه‌های الکترونیکی

محاوره مستقیم و چهره به چهره از راه دور

کنفرانس از راه دور

یافتن اشخاص مورد نظر در جهان

تلفن ودورنگار از طریق شبکه

رادیو از طریق شبکه

آموزش از راه دور

ارائه مدون اطلاعات فنی و علمی

اخبار مربوط به هنر ، ورزش ، سیاست ، تجارت و...

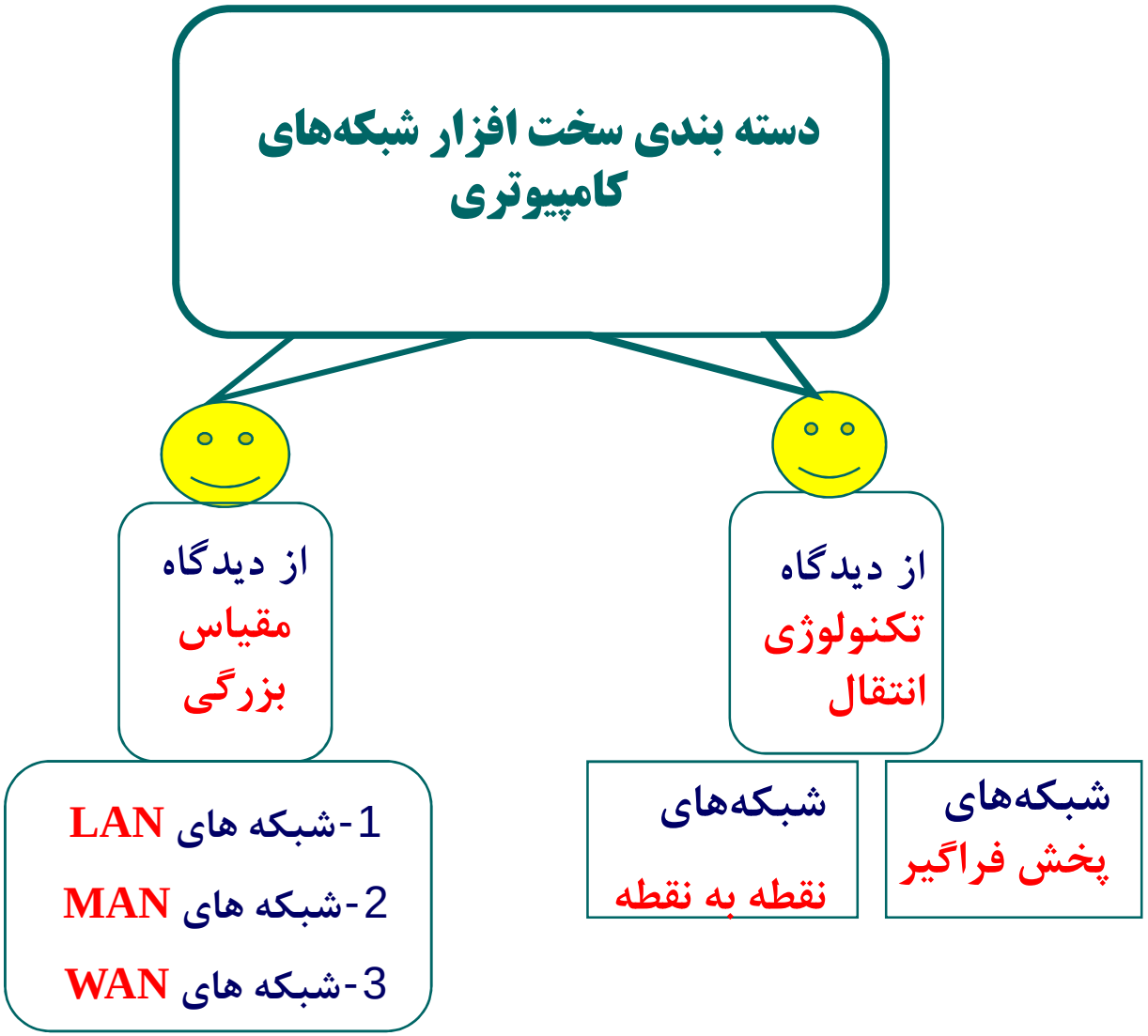
کاریابی و اشتغال

درمان از راه دور

خرید و فروش روزمره با استفاده از کارت اعتباری

انجمن‌های خیریه

مشاوره از راه دور


دسته بندی سخت افزار شبکه‌های کامپیوتری
از دیدگاه تکنولوژی انتقال
از دیدگاه مقیاس بزرگی
شبکه‌های پخش فراگیر
شبکه‌های نقطه به نقطه
1-شبکه های LAN
2-شبکه های MAN
3-شبکه های WAN

شبکه پخش فراگیر (Broadcast)

انتقال اطلاعات از طریق یک کانال فیزیکی مشترک توسط تمام ایستگاهها

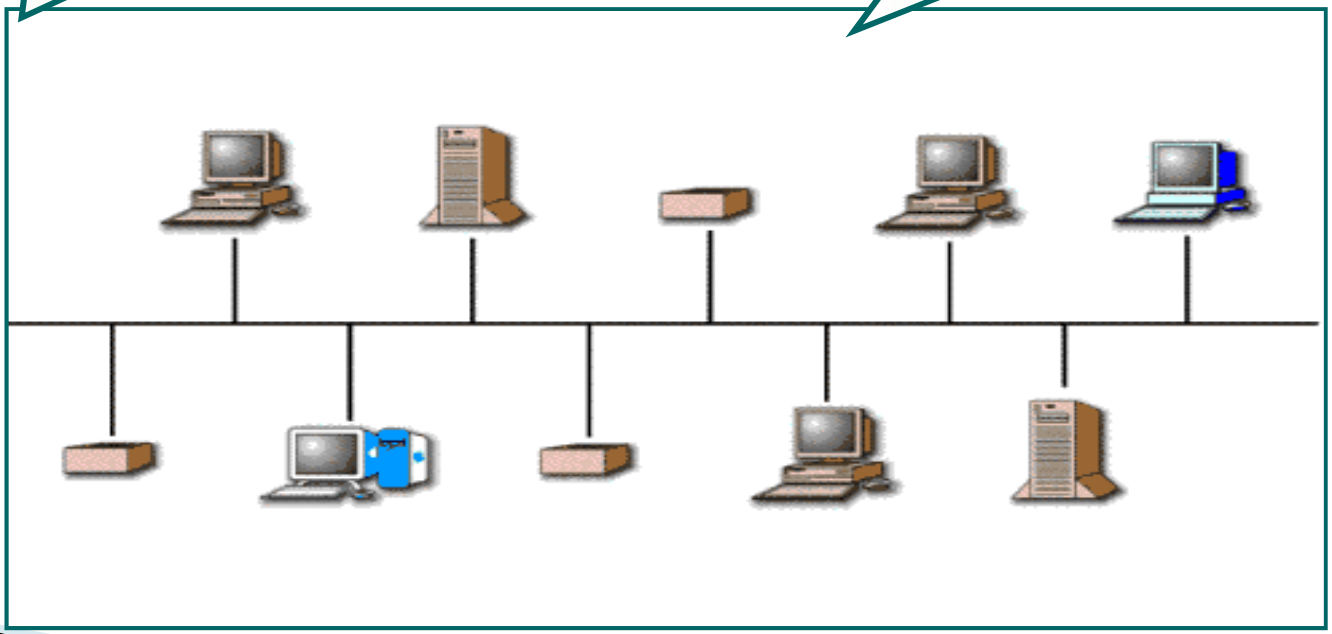
معایب شبکه‌های پخش فراگیر

1- مدیریت پیچیده کانال

2- امنیت پایین

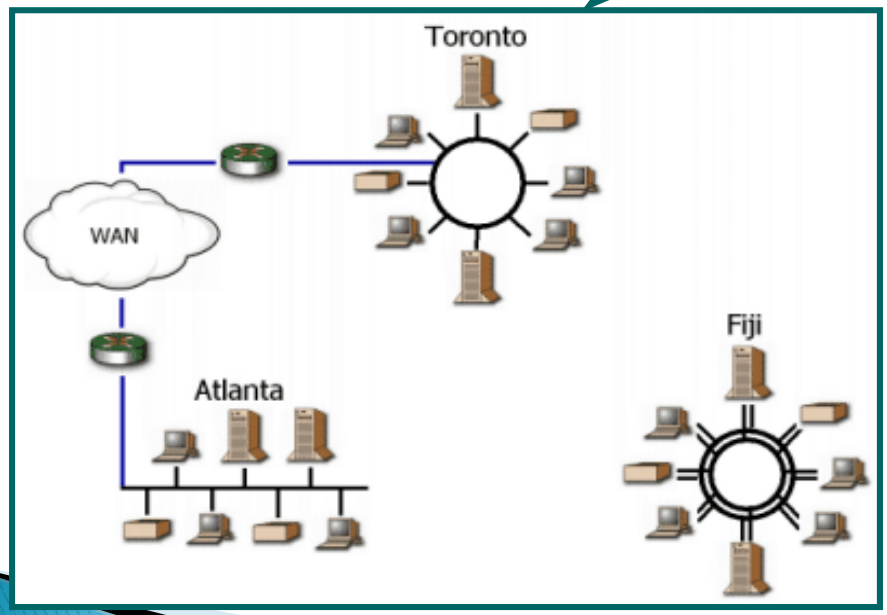
3- کارآیی نسبتا پایین

4- قابلیت اطمینان پایین



شبکه‌های نقطه به نقطه (point to point)

وجود فقط و فقط یک کانال فیزیکی و مستقیم
بین دو ماشین در شبکه



شبکه محلی LAN

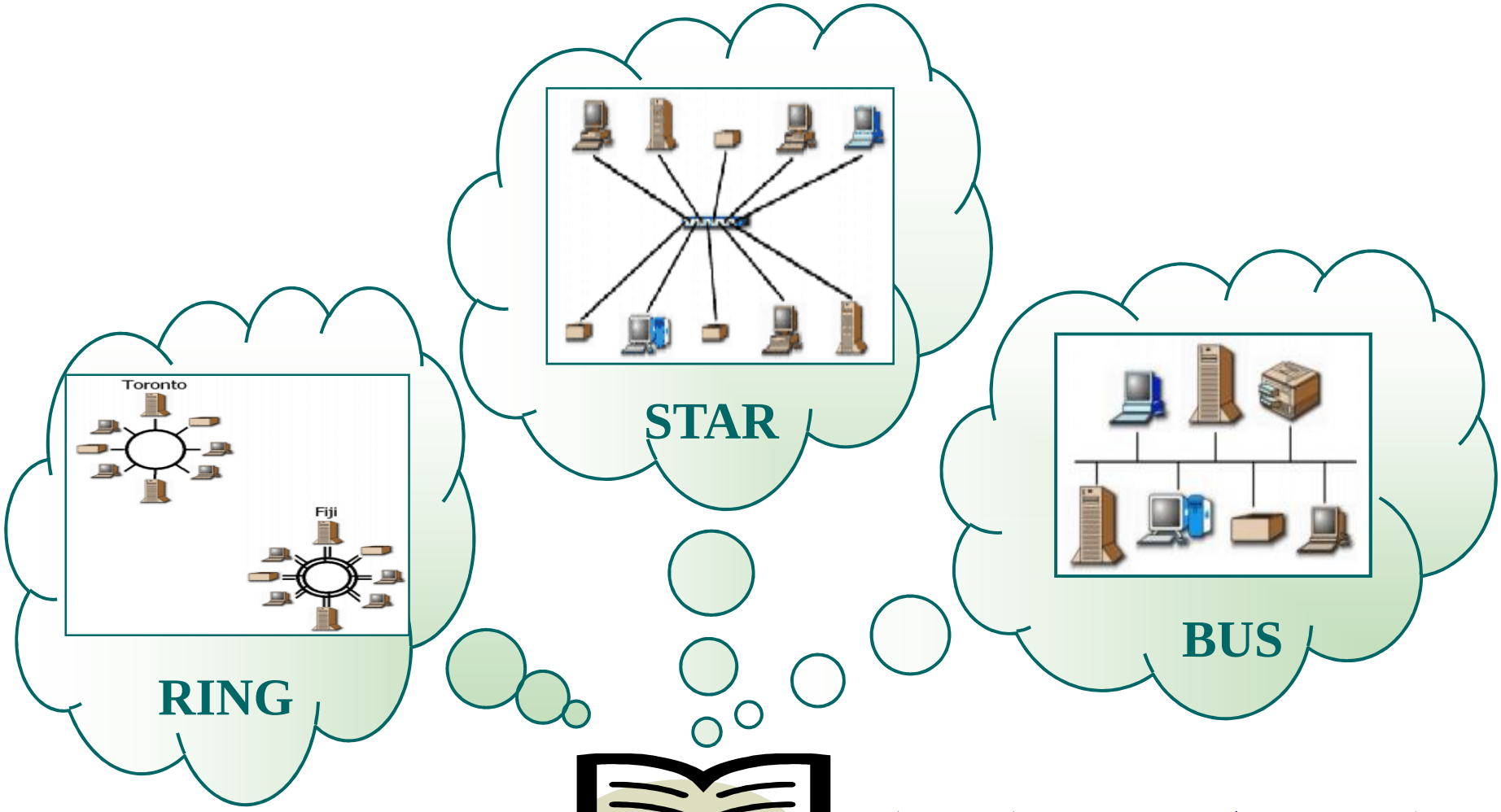
1- فواصل جغرافیایی محدود (حداکثر تا چند کیلومتر)

2- تعداد ایستگاهها کم

3- کوتاه بودن طول کانال انتقال

محاسن شبکه‌های LAN

1. افت سیگنال کم, نرخ خطای پایین, نرخ ارسال بالا و تأخیر انتشار بسیار ناچیز به دلیل کوتاه‌بودن طول کانال
2. مدیریت آسانتر شبکه به علت محدود بودن تعداد ایستگاهها
3. هزینه پایین نصب و راه‌اندازی این نوع شبکه.



انوع توپولوژی شبکه‌های محلی

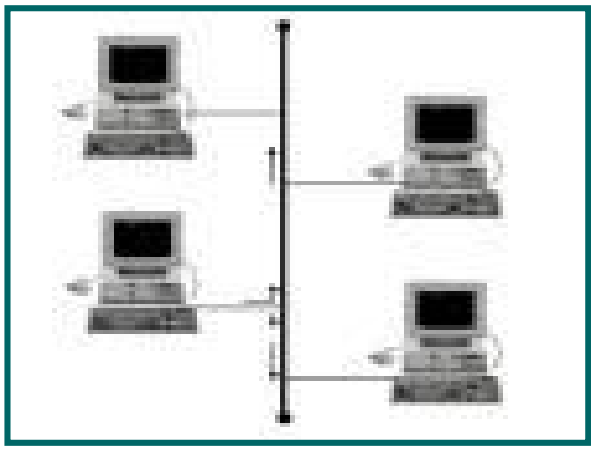
(انواع روش های اتصال ایستگاه های مختلف

به یکدیگر)

توپولوژی خطی - Bus

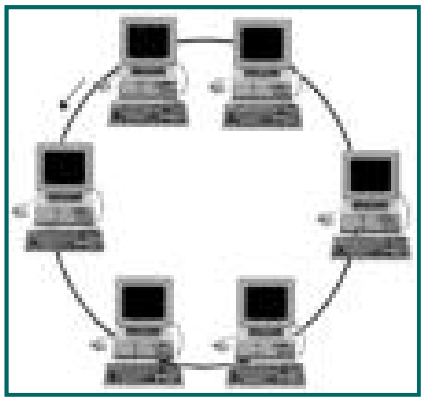
- اتصال تمام ایستگاهها از طریق یک کانال فیزیکی مشترک
- سادگی در نصب و راه اندازی و ارزان بودن

عیب : دشواری عیب یابی و رفع مشکلات



توپولوژی حلقه - (Ring)

- اتصال ایستگاهها در یک ساختار حلقوی به یکدیگر
- یکطرفه بودن ارتباط هر ایستگاه با ایستگاه بعدی خود
- دریافت بسته های اطلاعاتی توسط تمام ایستگاههای بین مسیر دو ایستگاه غیر مجاورجهت انتقال اطلاعات بین آن دو ایستگاه



توپولوژی حلقه - مزایا

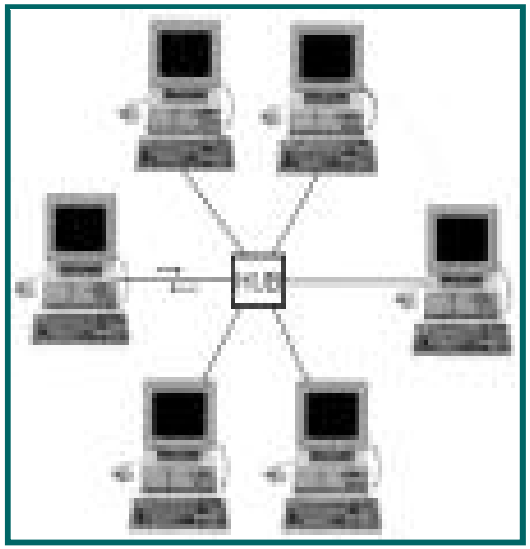
مزیت عمده توپولوژی Ring، پایین بودن افت سیگنال بخاطر بازسازی یا تقویت سیگنال توسط هر یک از ایستگاه‌های کاری است. در سایر توپولوژی‌ها، هنگامی که سیگنال در طول کابل حرکت می‌کند بخاطر تداخل خارجی ضعیف و ضعیف‌تر می‌شود. در این وضعیت اگر سیستم مقصد بیش از حد دور باشد، سیگنال غیرقابل استفاده خواهد بود. در عین حال، از آنجایی که هر یک از ایستگاه‌های کاری در یک توپولوژی Ringمسئولیت بازسازی سیگنال را بر عهده دارد، سیگنال هنگام رسیدن به مقصد قوی‌تر است و به ندرت نیازی برای ارسال مجدد آن وجود دارد.

توپولوژی حلقه - معایب

- بزرگترین مشکل توپولوژی Ring در این است که اگر یک کامپیوتر دچار نقص فنی شده یا یک کابل قطع شود، کل شبکه از کار خواهد افتاد. با این‌حال، فناوری‌های جدیدتر همیشه با این مشکل مواجه نیستند.
- از سوی دیگر، مکان‌یابی مشکلات در بعضی از پیکربندی‌های Ring بسیار دشوار است.
- مشکل دیگر توپولوژی Ring این است که اگر یک تغییر کابل‌کشی در شبکه اعمال شده یا یک ایستگاه را جابه‌جا کنید، قطع ارتباط موقت می‌تواند در عملکرد کل شبکه وقفه ایجاد کرده یا کل شبکه را از کار بیندازد.

توپولوژی ستاره -(Star)

- اتصال تمام ماشینهای شبکه توسط یک گره مرکزی
- گره مرکزی میتواند سوئیچ سریع یا هاب (Hub) ویا کامپیوتر باشد.



توپولوژی ستاره - مزایا

ü یکی از مزایای یک توپولوژی Star، مقیاس‌پذیری و سهولت اضافه شدن سیستم‌های بیشتر به شبکه است. اگر نیاز دارید که ایستگاه کاری دیگری در یک توپولوژی Star به شبکه اضافه شود، کافی است سیستم را به یک درگاه آزاد روی هاب متصل کنید.

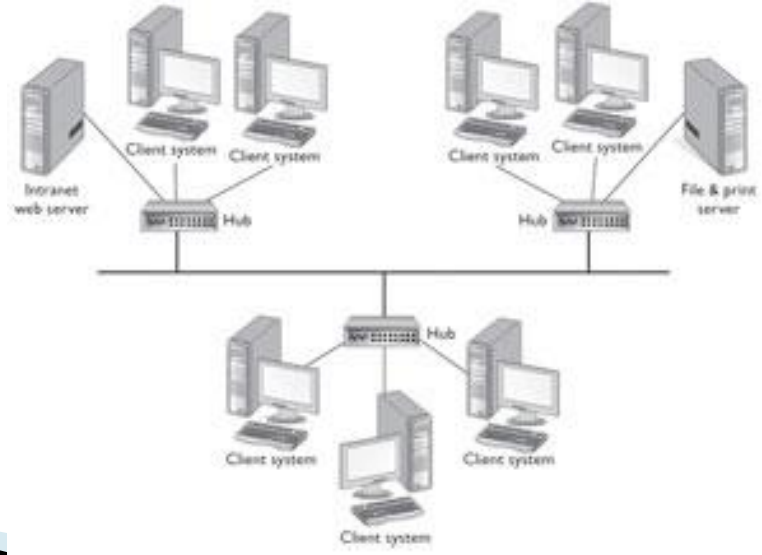
ü مزیت دیگر توپولوژی Star، این واقعیت است که اگر یک قطعی در کابل ایجاد شود، تنها بر سیستمی تاثیر می‌گذارد که به همان کابل متصل است. شکل 5 یک هاب را با چند درگاه آزاد نشان می‌دهد.

توپولوژی ستاره - معایب

- اگر ابزار مرکزی در یک شبکه Starاز کار بیفتد، کل شبکه از کار خواهد افتاد و به همین دلیل ما هنوز با یک نقطه مرکزی خرابی مواجه هستیم. با این‌حال، عیب‌یابی و رفع مشکل در این وضعیت بسیار آسان‌تر از تلاش برای پیدا کردن یک قطعی کابل در توپولوژی Busخواهد بود.
- نقیصه دیگر توپولوژی Star، هزینه بالای آن است. برای اتصال هر ایستگاه کاری به شبکه، شما باید مطمئن شوید که یک درگاه آزاد روی ابزار مرکزی وجود دارد. در عین حال، شما به یک کابل برای اتصال ایستگاه‌کاری مورد نظر به ابزار مرکزی نیاز خواهید داشت. امروزه مشکل هزینه به‌خاطر کاهش قیمت‌های ابزارهایی مانند هاب یا سوییچ بسیار کم‌رنگ‌تر شده است.

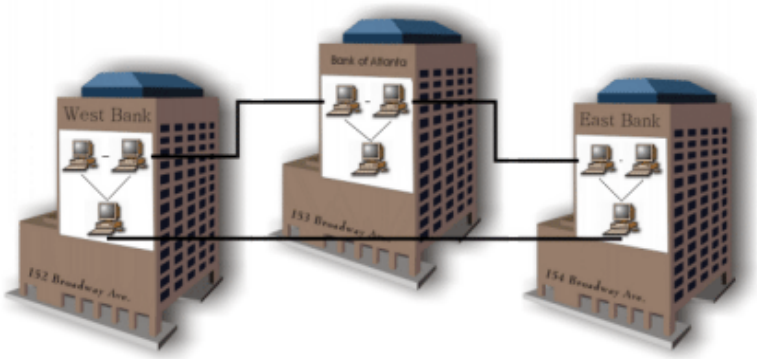
توپولوژی ترکیبی -(Hybrid)

بسیاری از شبکه‌ها مجموعه‌ای از توپولوژی های مختلف را در قالب یک توپولوژی ترکیبی پیاده‌سازی می‌کنند. مانند، توپولوژی **Star-Bus**



شبکه های بین شهری (MAN)

برای ایجاد شبکه در سطح یک منطقه وسیع درحد یک شهـر یا اتصال چندین شبکه محلی ، از شبکه MAN استفـاده مـی‌شود . این شـبکه تکنولوژی و توپولوژی مشابه با شبکه‌های محلی دارد. بدلیل طول زیاد کانال معمولا از فیبر نوری استفاده می‌شود.

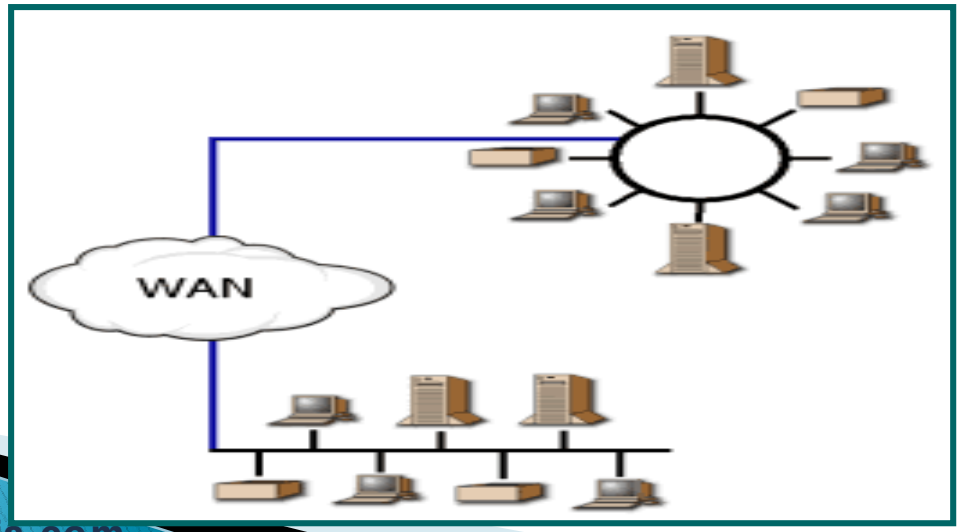


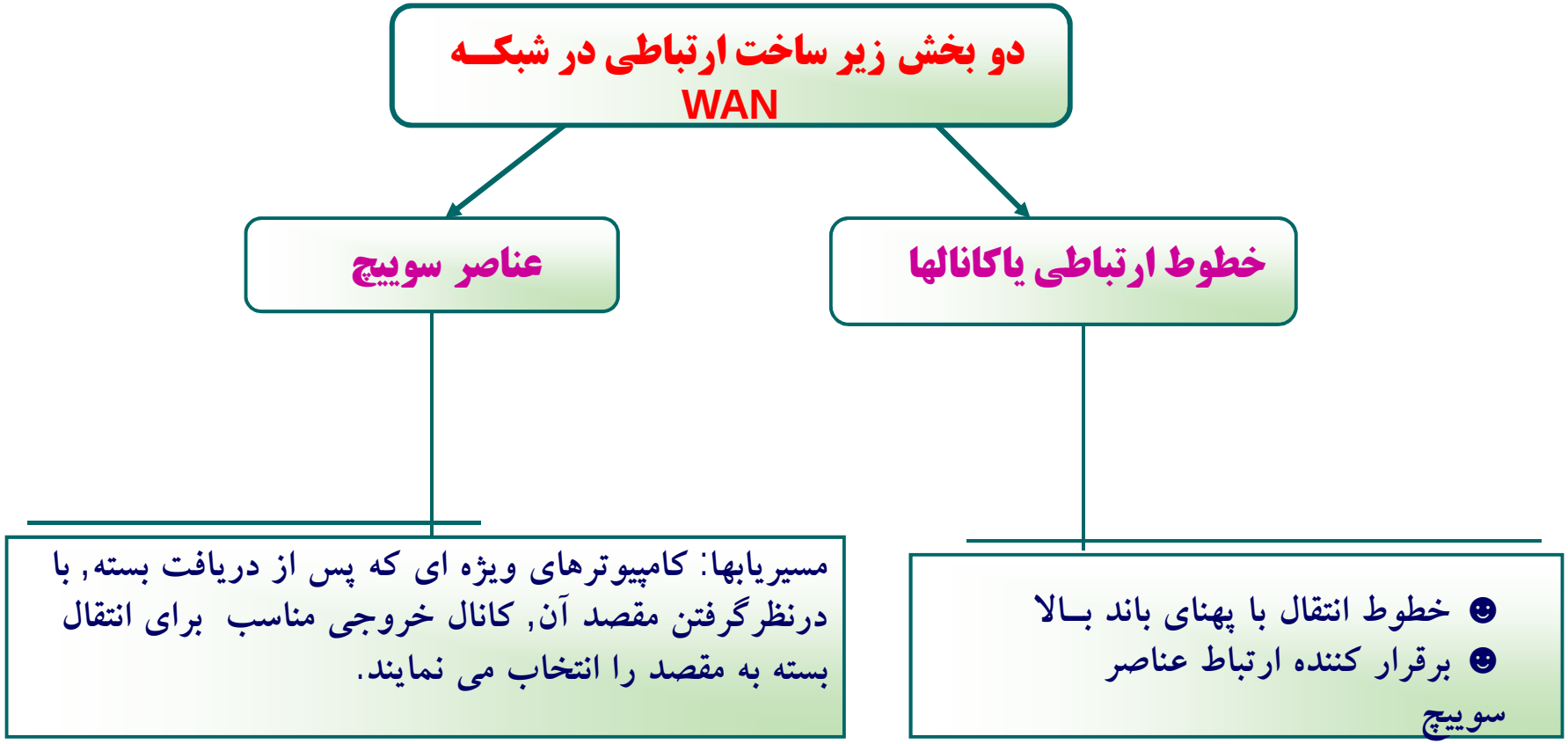
شبکه‌های گسترده (WAN)

- پیاده سازی در گستره جغرافیایی یک کشور یا جهان
- اتصال شبکه های محلی و بین شهری
- ساختار ناهمگون

توپولوژیهای مختلف شبکه های محلی

تنوع در سخت افزار و نرم افزار ماشینهای موجود دراین شبکه ها




دو بخش زیر ساخت ارتباطی در شبکـه WAN
عناصر سوییچ
خطوط ارتباطی یاکانالها
مسیریابها: کامپیوترهای ویژه ای که پس از دریافت بسته, با درنظرگرفتن مقصد آن, کانال خروجی مناسب برای انتقال بسته به مقصد را انتخاب می نمایند.
☻ خطوط انتقال با پهنای باند بـالا
☻ برقرار کننده ارتباط عناصر سوییچ

شبکه های بی سیم (Wireless)

موارد استفاده:

- ایجاد شبکه‌ای با وجود ایستگاههای متحرک
- استفاده در مکانهایی که کابل‌کشی در آن مقرون به صرفه و یا عقلانی نیست.

مزایا

- ساده بودن نصب و راه اندازي اين نوع شبکه

معایب

- نرخ ارسال و دریافت پایین
- نرخ خطا نسبتاً بالا
- امنیت اطلاعات کم

انواع شبکه های بی سیم

ارتباطات داخل سیستمی

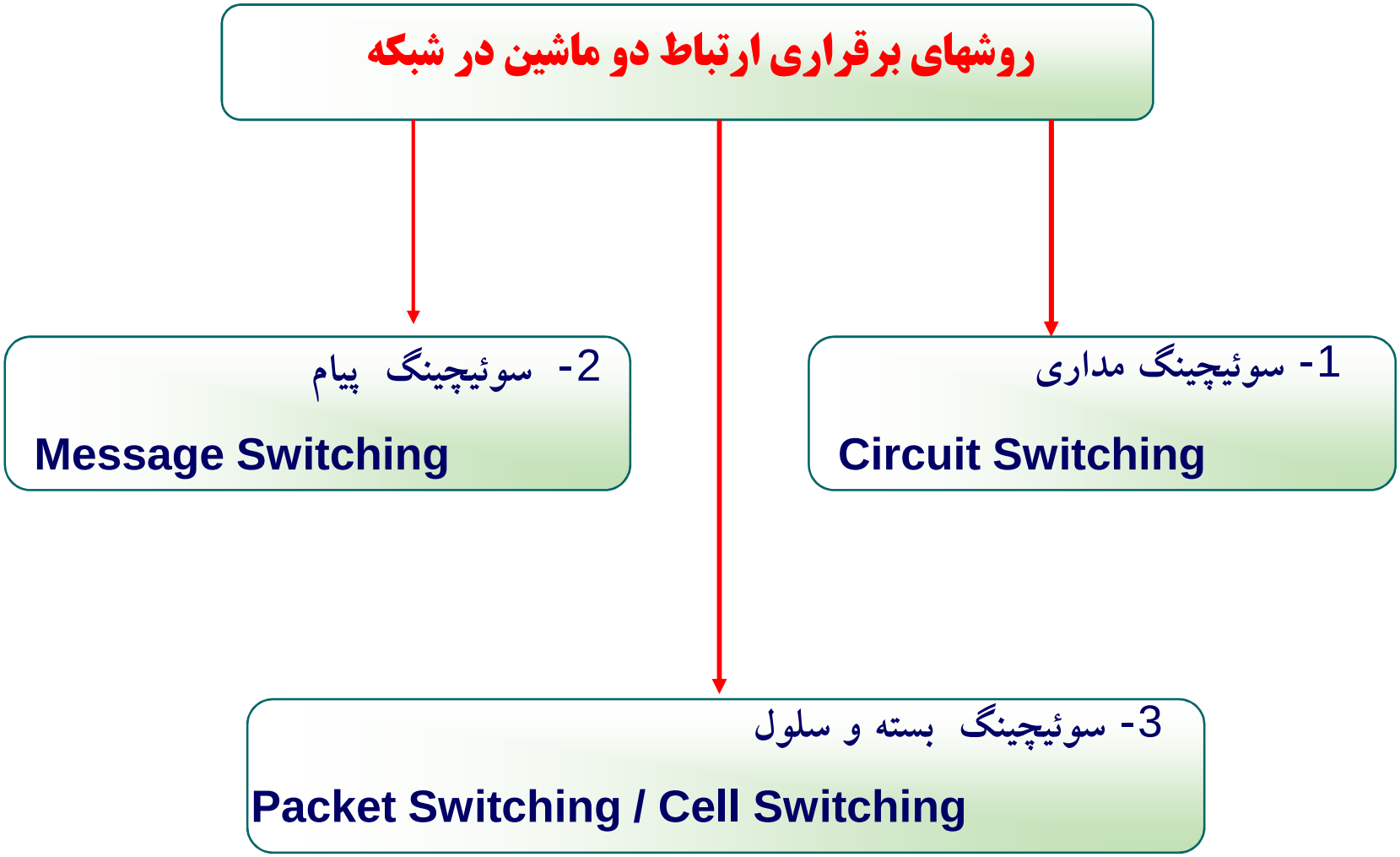
مثل كي بورد و ماوس بي سيم
اين مزيت باعث مي شو د دستگاه ها با قرار گرفتن در برد امواج بتوانند با يكديگر ارتباط برقرار كنند.

LANبی سیم

LAN نوع ديگر ارتباطات بي سيم است كه در آن هر كامپيوتر داراي يك مودم راديويي و يك آنتن است كه بدينوسيله با كامپيوترهاي ديگر ارتباط برقرار مي كند

WANبی سیم

- مانند شبكه تلفن همراه
- برد بيشتر و نرخ انتقال داده كمتر نسبت به LAN بي سيم


روشهای برقراری ارتباط دو ماشین در شبکه
1- سوئیچینگ مداری
Circuit Switching
2- سوئیچینگ پیام
Message Switching
3- سوئیچینگ بسته و سلول
Packet Switching / Cell Switching

1 - سوئیچینگ مداری

Circuit Switching

لزوم برقراری اتصال فیزیکی بین مبدأ و مقصد جهت انتقال اطلاعات

معایب

- نیاز به زمان قابل توجهی برای برقراری ارتباط بین فرستنده و گیرنده
- عدم امکان برقراری ارتباط توسط ماشینهای دیگر با دو ماشین فرستنده و گیرنده هنگام اشغال بودن کانال توسط دو ماشین

2 - سوئیچینگ پیام

Messeage Switching

- مختص انتقال دادهای دیجیتال
- اتصال دائمی هرایستگاه با مرکز سوئیچ خود
- اضافه نمودن اطلاعات لازم به داده ها قبل از ارسال آن به مرکز سوئیچ توسط ایستگاه فرستنده
- دریافت کامل پیام توسط هر مرکز سوئیچ و انتخاب کانال خروجی مناسب بر اساس آدرس گیرنده موجود در داده

مشکل سوئیچینگ پیام

عدم محدودیت طول پیام

- بالا بودن حافظه‌های موجود درهر مرکز سوئیچ
- ارسال مجدد داده‌ها در صورت خرابی یک بیت در پیام
- تأخیر زیاد در رسیدن پیام

مزایا

- بسیار سریع و کارآمد
- عدم اشغال کانال

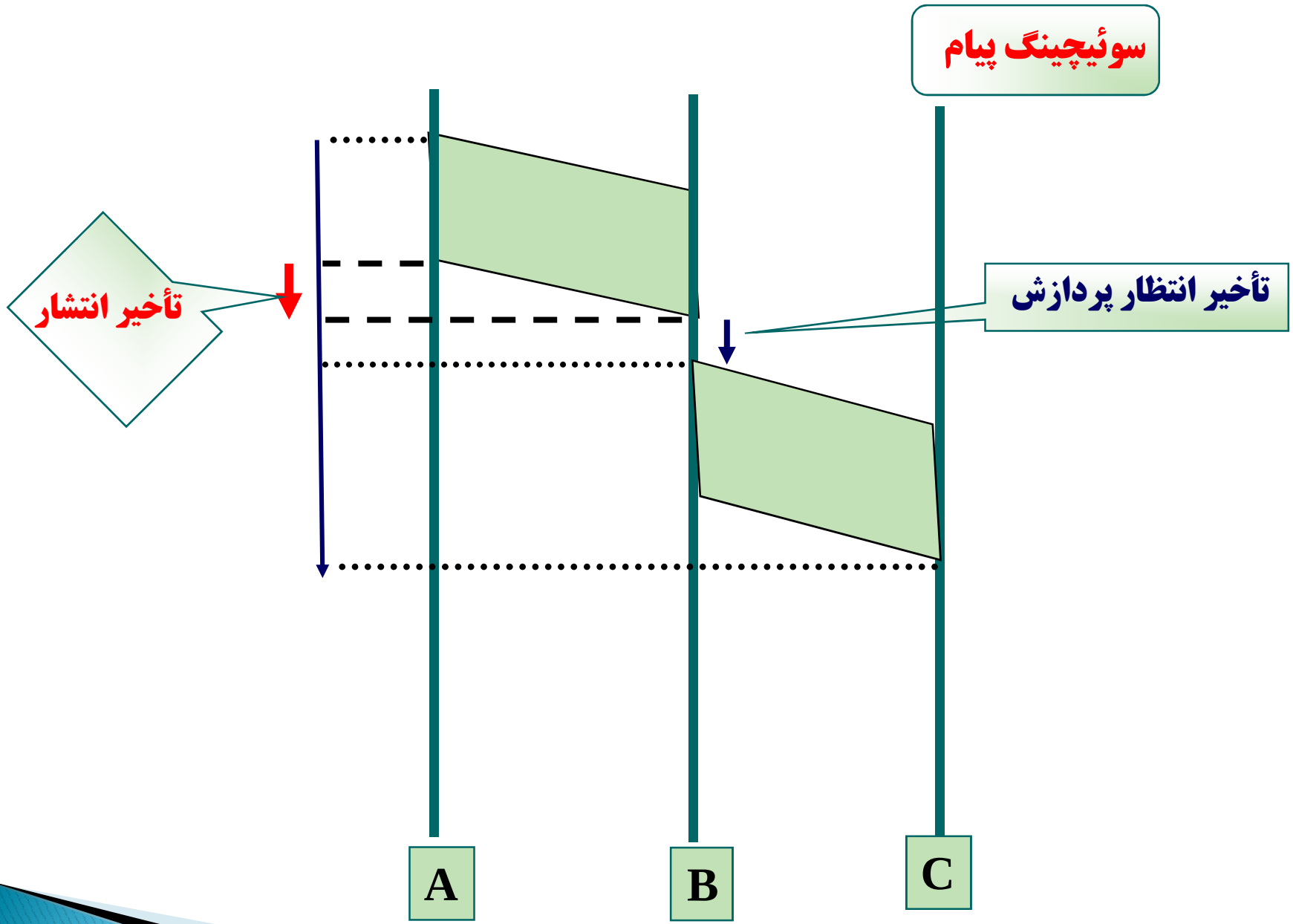
3 - سوئیچینگ بسته و سلول

Packet / Cell Switching

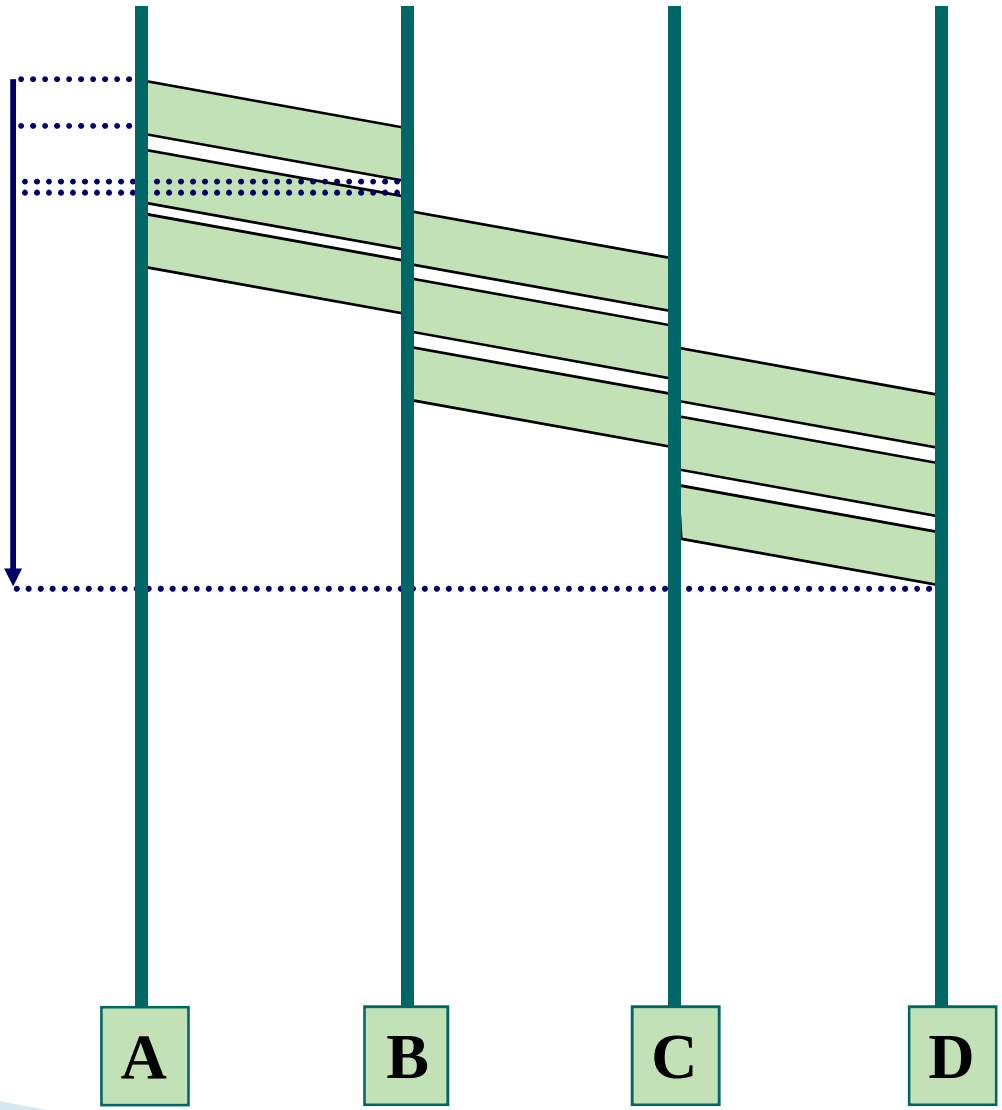
شکستن پیام توسط ایستگاه فرستنده به قطعات کوچکتری به نام **بسته** و ارسال هر بسته به همراه اطلاعات لازم برای بازسازی آن به طور جداگانه به مراکز سوئیچ

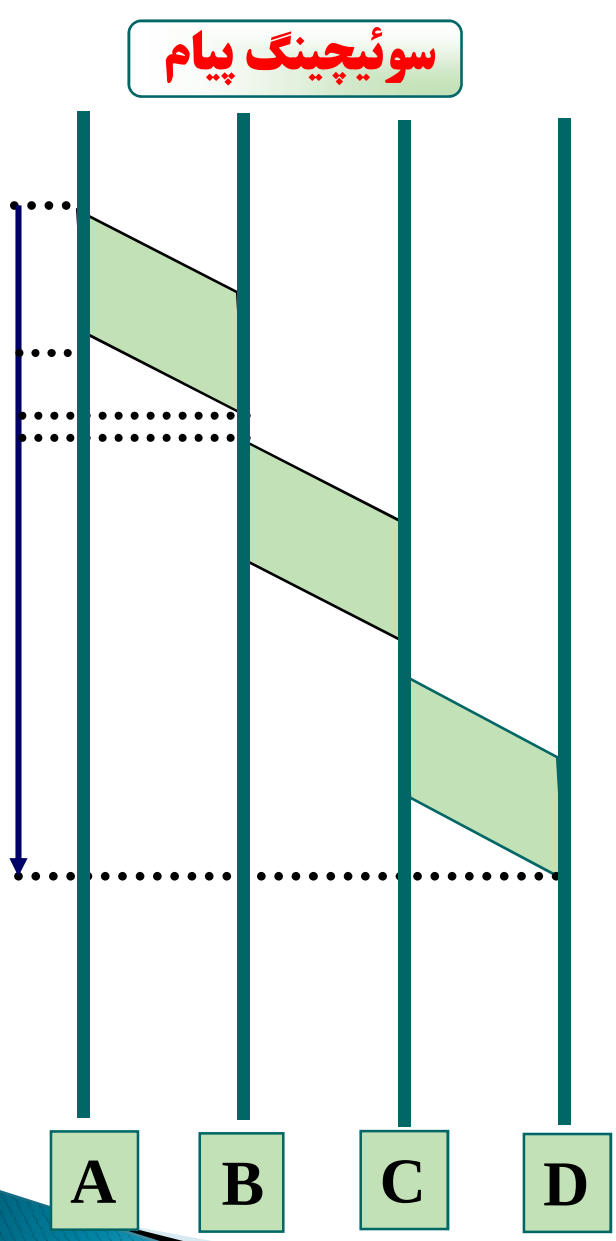
مقایسه دو روش سوئیچینگ پیام وبسته / سلول

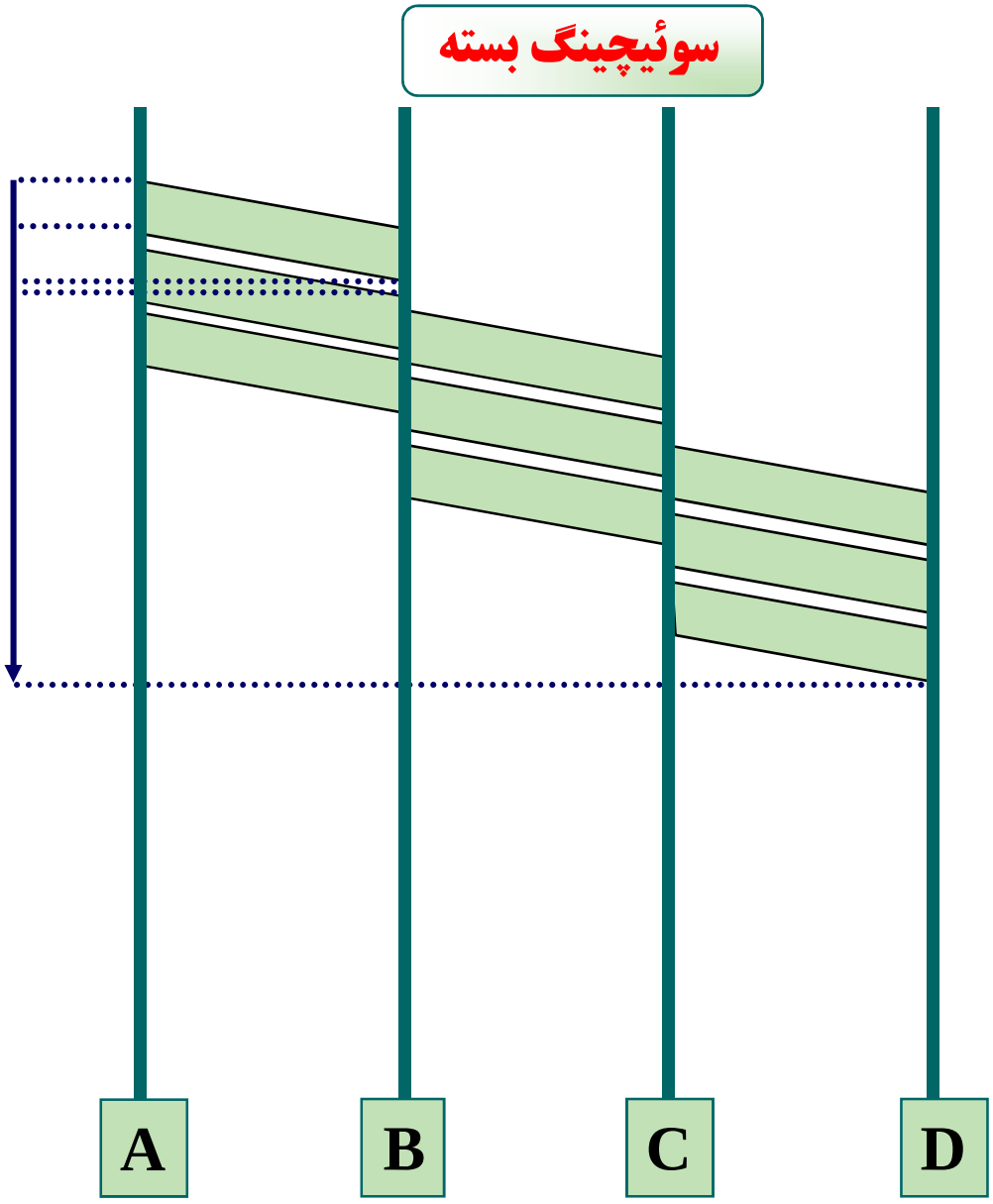
- مجموع تأخیر کمتر در روش سوئیچینگ بسته نسبت به روش سوئیچینگ پیام
- نیاز به فضای حافظه کمتر و قابل تأمین در هر مرکز سوئیچ در روش سوئیچینگ بسته
- عدم تأثیر خرابی یک بسته در کل پیام ارسالی و نیاز به ارسال مجدد فقط همان بسته


سوئیچینگ پیام
تأخیر انتشار
تأخیر انتظار پردازش
A
B
C

سوئیچینگ بسته



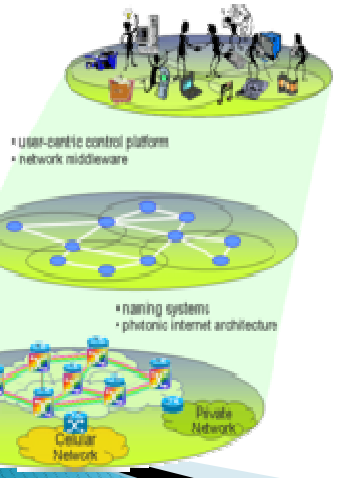




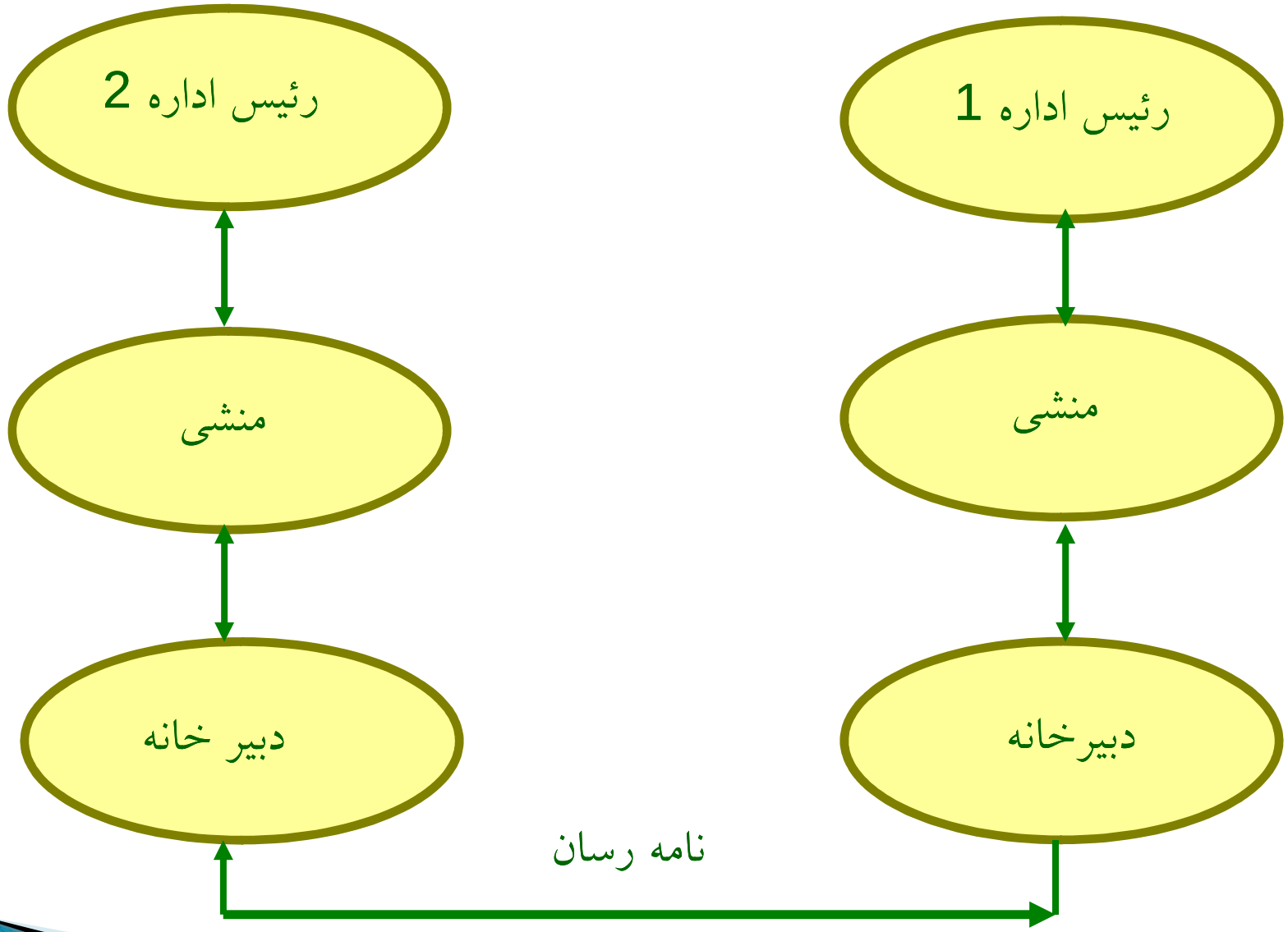
زمانبندی تأخیر در روشهای سوئیچنگ پیام و بسته

معماری شبکه

جهت برقراری ارتباط و تبادل اطلاعات بین دو کامپیوتر در شبکه باید یک سری عملیات در جهت کاهش پیچیدگی شبکه و افزایش انعطاف پذیری شبکه صورت گیرد. عملیات یک شبکه را به صورت لایه های مختلفی تقسیم بندی می کنند .

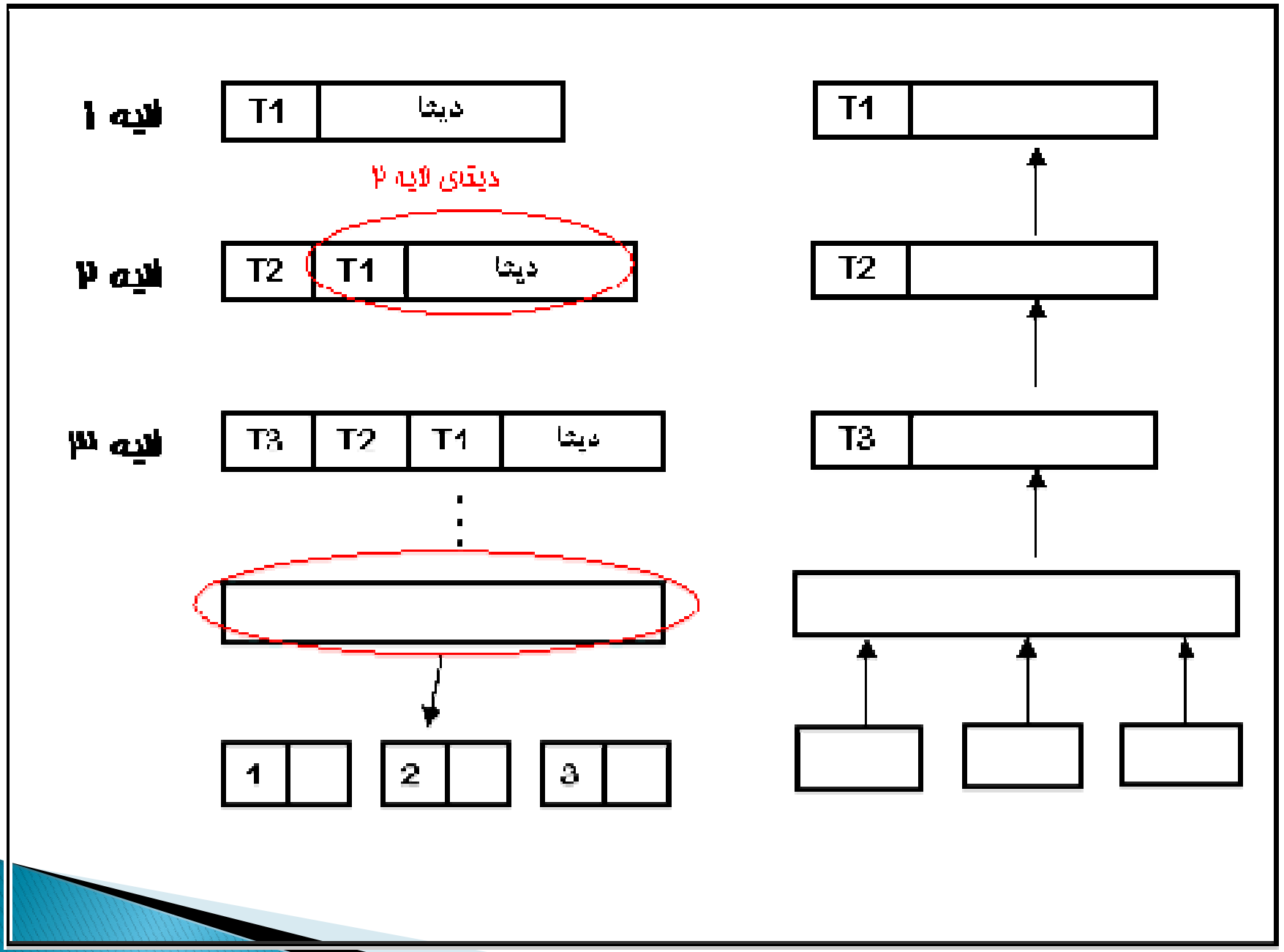


- Fragmentation(قطعه قطعه شدن)
- Assemble


رئیس اداره 2
رئیس اداره 1
منشی
منشی
دبیر خانه
دبیرخانه
نامه رسان

Fragmentation(قطعه قطعه شدن)

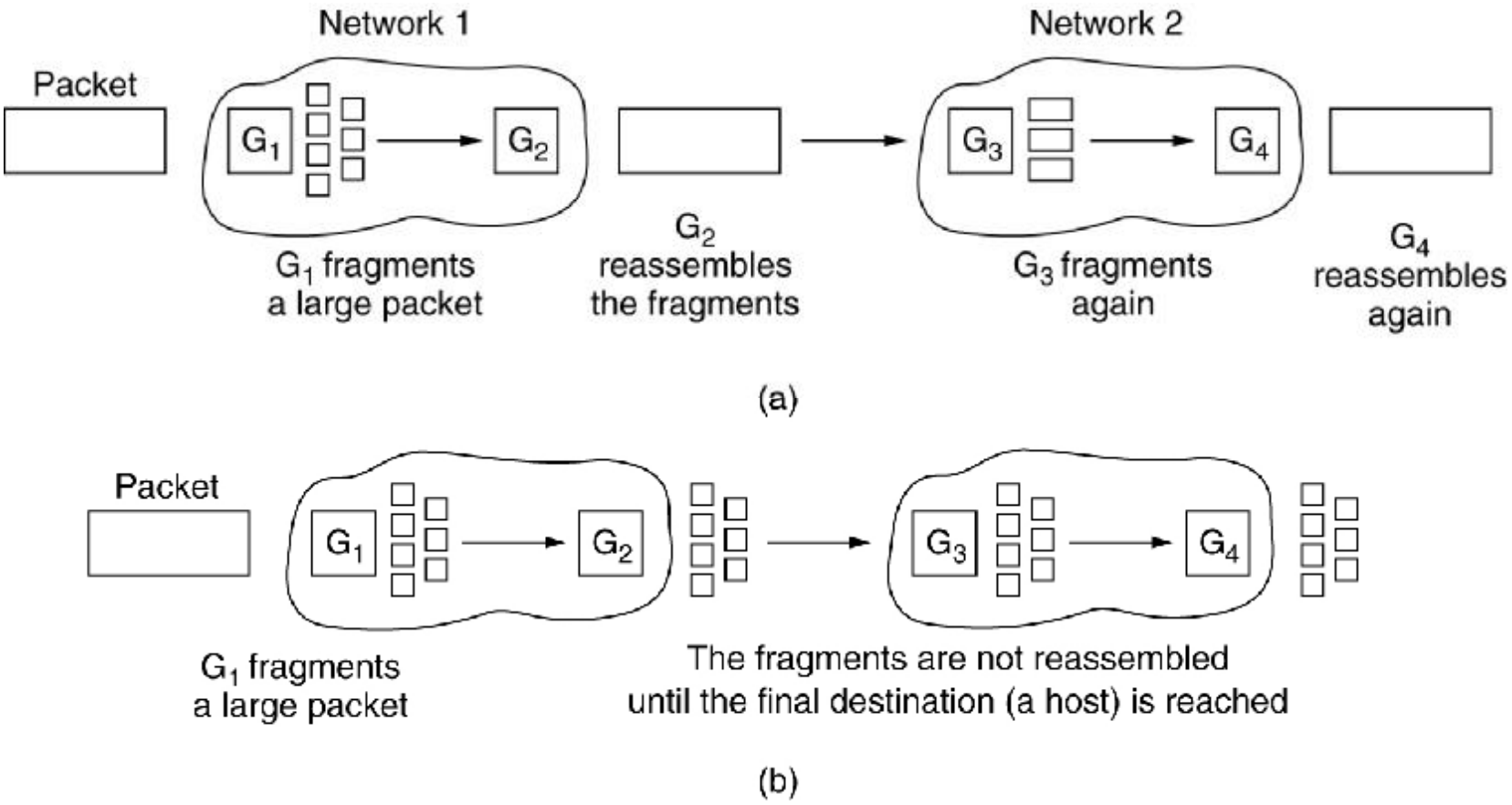
اطلاعات از یک سطح به سطح بعد در صورت بزرگتر بودن از سایز مجاز باید به قطعات کوچکترتقسیم شوند تا بتوانند انتقال یابند، به این عمل قطعه قطعه شدن گوییم .


لایه ۱
T1
دیتا
دیتای لایه ۲
لایه ۲
T2
T1
دیتا
لایه ۳
T3
T2
T1
دیتا
1
2
3
T1
T2
T3

معماری شبکه ...

- اطلاعات ایجاد شده در بالا ترین لایه شبکه برای ارسال به شبکه باید از لایه های مختلف از بالا به پائین عبور کند تا به پائین ترین لایه برسد و ازطریق آن واردزیر شبکه گردد هر لایه اطلا عات کنترلی خود را به پیغام اضافه می کند.
- به مجموع لایه ها و پروتکل های شبکه معماری شبکه گفته می شود. با استفاده از مشخصات و اطلاعات از معماری شبکه می توان نرم افزارها و سخت افزارهای هرلایه را طراحی و تولید کرد.

Fragmentation(قطعه قطعه شدن)



(a)Transparent fragmentation. (قطعه قطعه شدن شفاف)

(b) Nontransparent fragmentation.(قطعه قطعه شدن غیر شفاف)

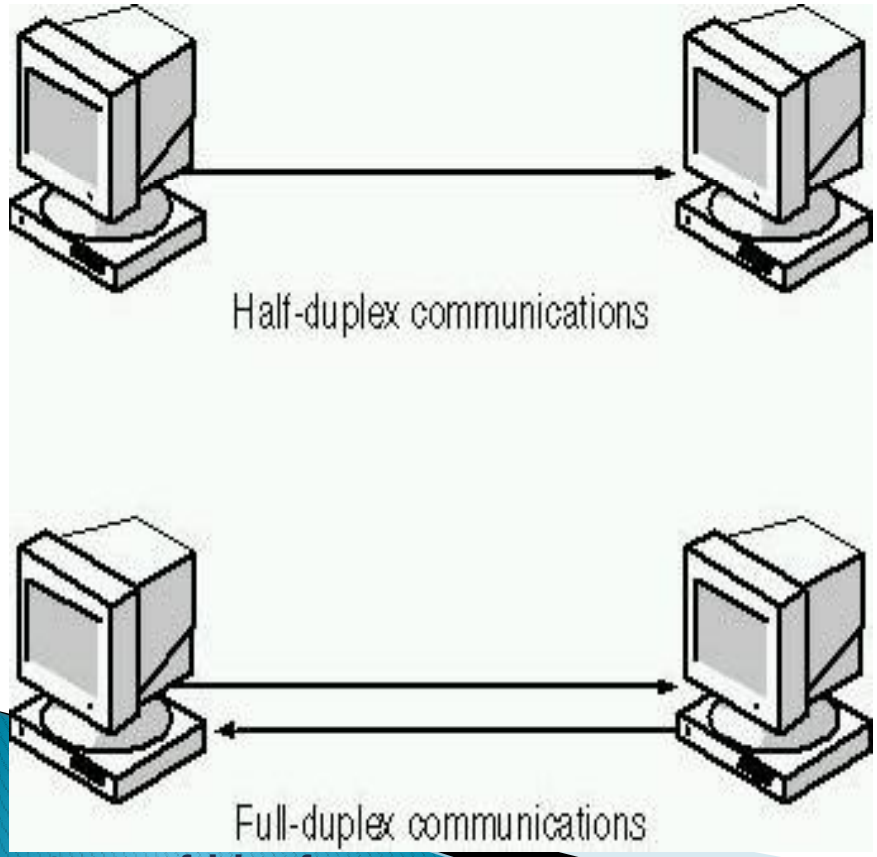
انواع ارتباط میان دو ایستگاه

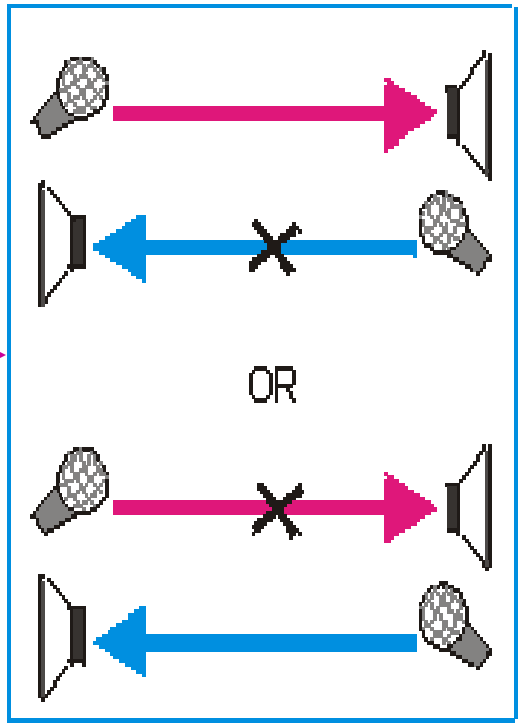
- ارتباط یکطرفه - Simplex:
یکطرف همیشه گیرنده و یکطرف همیشه فرستنده

- ارتباط دوطرفه غیرهمزمان - Half duplex
هر دو ماشین هم می‌توانند فرستنده باشند و هم گیرنده ولی نه بصورت همزمان

- ارتباط دوطرفه همزمان - Full duplex
ارتباط دو طرفه همزمان مانند خطوط ماکروویو

Simplex communication





به نام خدا

طراحی و پیاده سازی زیر ساخت شبکه های کامپیوتری

مدرس: مهندس ملیحه امینی

مدل مرجع OSI (Open System Interconnection)

این مدل بر مبنای قراردادی است که سازمان استانداردهای جهان **ISO**به عنوان اولین مرحله از استاندارد سازی قراردادهایی که در لایه های مختلف مورد استفاده قرار می گیرند، ایجاد کرد (دی و زیمر من ،1983). این مدل در سال 1995 بازبینی شد (دی ، 1995). نام این مدل **OSI**انتخاب شد، زیرا با اتصال سیستم های باز سروکار دارد. منظور از سیستم های باز سیستم هایی است که برای ارتباط با سایر سیستم ها، باز هستند. برای اختصار، آن را **OSI**می نامیم.

مدل OSIهفت لایه دارد.

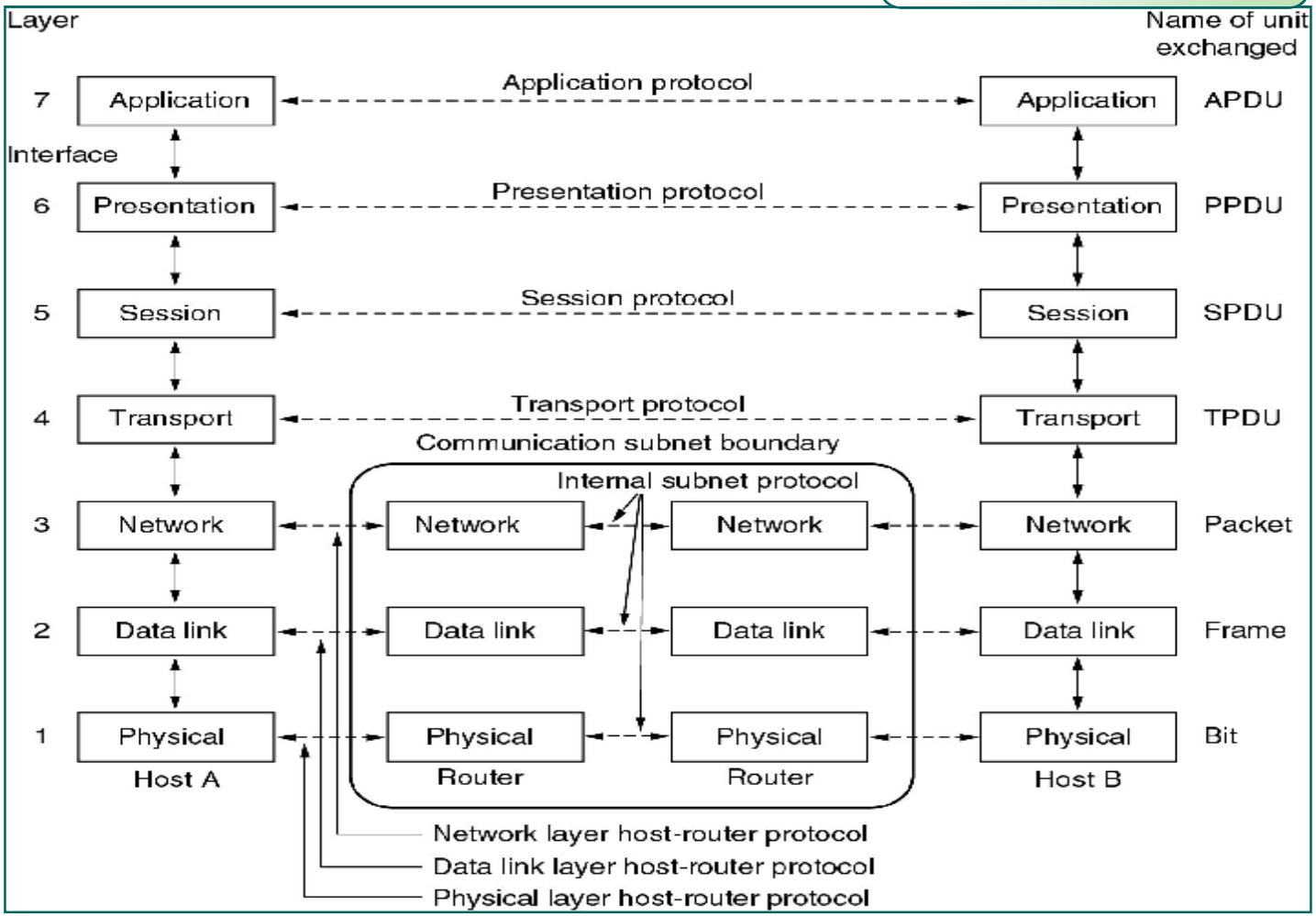
اصولی که منجر به این هفت لایه شده اند عبارتند از :

1. وقتی نیاز به سطوح مختلفی از انتزاع است، لایه ای باید ایجاد شود.
2. هر لایه باید وظیفه مشخصی داشته باشد.
3. وظیفه هر لایه باید با در نظر گرفتن قراردادها و استاندارد جهانی انتخاب گردد.
4. مرزهای لایه باید برای به حداقل رساندن جریان اطلاعات از طریق واسط ها انتخاب شوند.
5. تعداد لایه ها باید آن قدر زیاد باشد که نیازی به قرار دادن وظایف متمایز در یک لایه نباشد و به اندازه کافی کوچک باشد تا معماری نامناسب نباشد

مدل هفت لایه‌ای OSI از سازمان استاندارد جهانی ISO

- لایه فیزیکی Physical layer
- لایه پیوند داده‌ها Data link layer
- لایه شبکه Network layer
- لایه انتقال Transport layer
- لایه جلسه Session layer
- لایه ارائه (نمایش) Presentation layer
- لایه کاربرد Application layer

مدل هفت لایه‌ای OSI



لایه فیزیکی Physical Layer

وظایف :

1.ارسال بیتهای خام صفر و یک

2.تعیین سطوح ولتاژ برای صفر و یک

لایه پیوند داده - Data Link Layer

وظایف :

- به مقصد رساندن داده‌ها روی یک کانال انتقال بدون خطا و مطمئن با استفاده از مکانیزمهای کشف و کنترل خطا.
- شکستن اطلاعات ارسالی از لایه بالاتر به واحدهای استاندارد و کوچکتر و مشخص نمودن ابتدا و انتهای آن از طریق نشانه‌های خاصی بنام **Delimiter**.
- کشف خطا از طریق اضافه کردن بیتهای کنترل خطا
- کنترل جریان یا تنظیم جریان ارسال فریمها (مکانیزمهای هماهنگی بین مبدأ و مقصد)
- اعلام وصول یا عدم رسیدن داده‌ها به فرستنده
- وضع قراردادهائی برای جلوگیری از تصادم سیگنالهای ارسالی (این قراردادها در زیرلایه‌ای بنام **MAS** تعریف شده است)
- کنترل سخت‌افزار لایه فیزیکی

لایه شبکه

وظایف:

1.مسیریابی
2.کنترل تراکم
3.ارتباط بین شبکه ای

- در شبکه های محلی و انتشار همگانی معمولا از این لایه استفاده نمی شود. وظیفه لایه شبکه پیدا کردن مسیر ها و انتخاب بهترین آنهاست.
- ارتباطات در این لایه به صورت نقطه به نقطه صورت می گیرد .

لایه انتقال

1.ارسال بسته های لایه های بالا تر به مقصد
2. این لایه برای سرویس دهی به لایه بالایی(جلسه)وموظف به برقراری اتصالهای مختلف با مقصد است.

لایه جلسه Session Layer

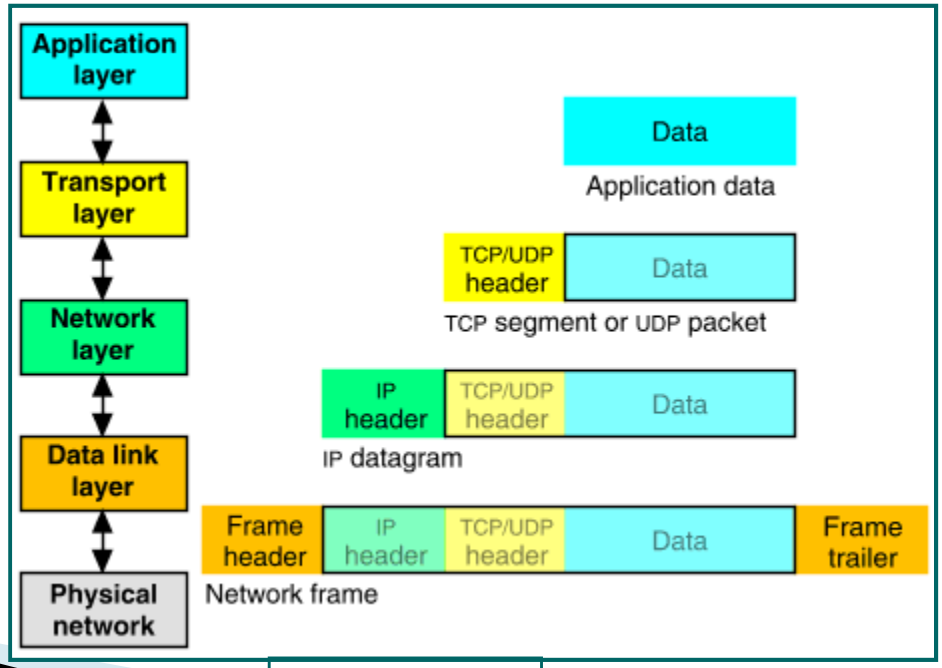
- برقراری و مدیریت یک جلسه
- شناسائی طرفین
- مشخص نمودن اعتبار پیامها
- اتمام جلسه‌ها
- حسابداری مشتریها

لایه ارائه (نمایش)

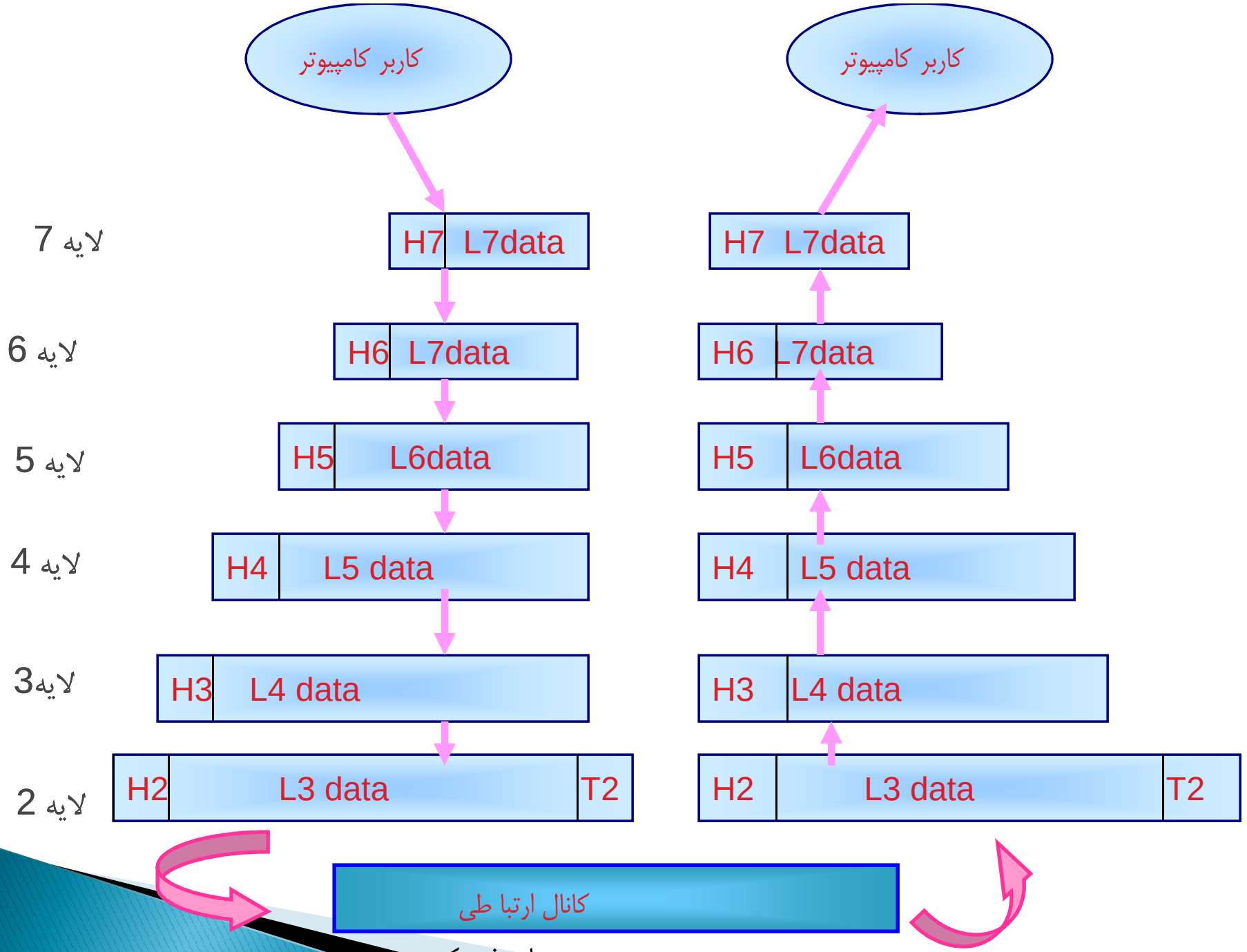
- فشرده‌سازی فایل
- رمزنگاری برای ارسال داده‌های محرمانه
- رمزگشائی
- تبدیل کدها به یکدیگر هنگام استفاده دو ماشین از استانداردهای مختلفی برای متن

لایه کاربرد Application Layer

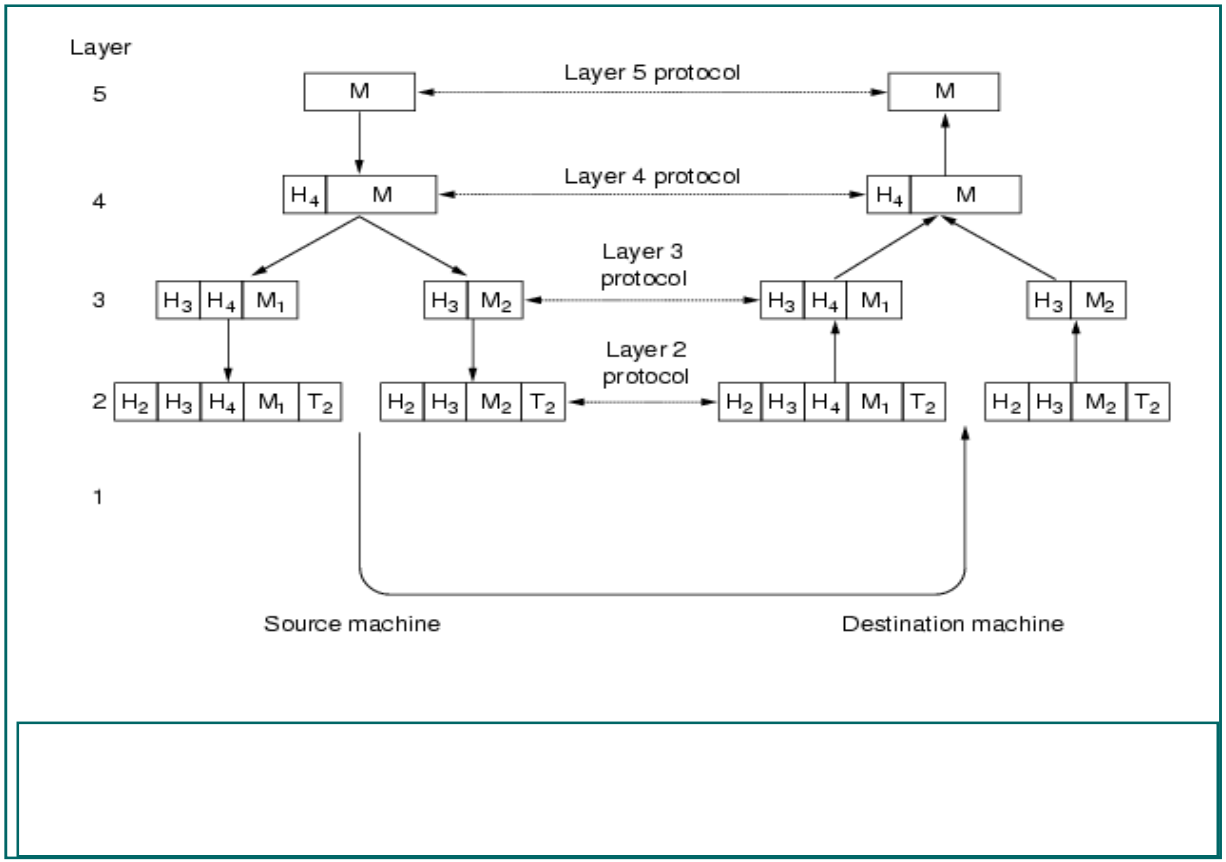
وظیفه:
در اختیار قرار دادن نرم افزارهای مختلف
برای کاربران شبکه



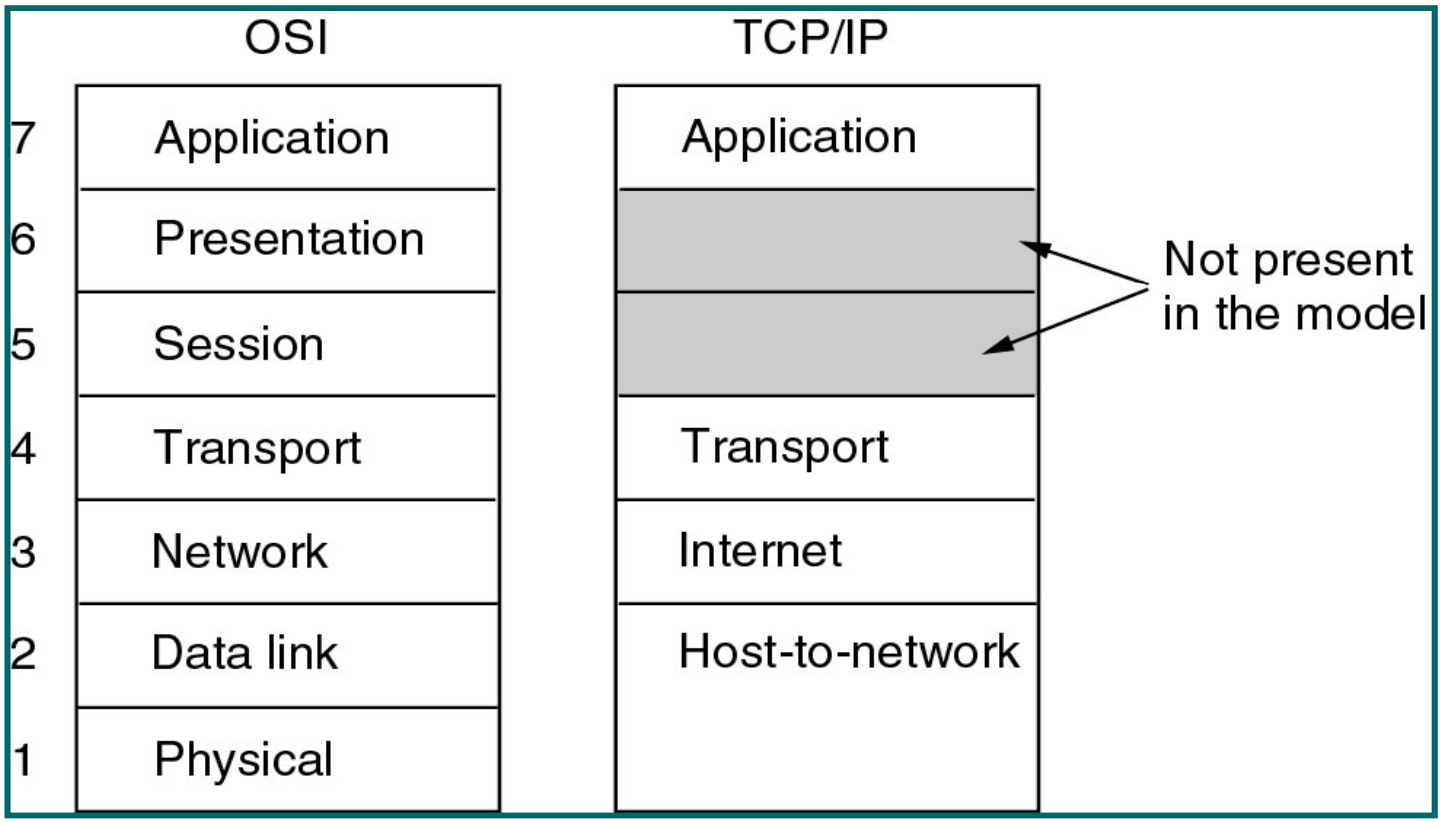
مدل OSI


کاربر کامپیوتر
کاربر کامپیوتر
لایه 7
لایه 6
لایه 5
لایه 4
لایه3
لایه 2
H7 L7data
H7 L7data
H6 L7data
H6 L7data
H5 L6data
H5 L6data
H4 L5 data
H4 L5 data
H3 L4 data
H3 L4 data
H2 L3 data T2
H2 L3 data T2
کانال ارتبا طی
رسانه فیزیک

روند حذف و اضافه شدن سرآیند در هر لایه



مدل چهارلایه‌ای TCP/IP



لایه‌های مدل TCP/IP

لایه‌ها	نامهای معادل در برخی از کتب
لایه کاربرد Application layer	• لایه سرویسهای کاربردی
لایه انتقال Transport layer	• لایه ارتباط میزبان به میزبان (Host to Host) • لایه ارتباط عناصر انتهائی (End to End Connection)
لایه شبکه Network layer	• لایه اینترنت • لایه ارتباطات اینترنت
لایه دسترسی به شبکه Network Interface	• لایه میزبان به شبکه (Host to Network) • لایه رابط شبکه

لایه اول از مدل TCP/IP : لایه واسط شبکه

تعریف لایه‌های استاندارد سخت‌افزار، نرم‌افزارهای راه‌انداز و پروتکلهای شبکه در این لایه. پروتکلهائی که در لایه اول از مدل TCP/IP تعریف می‌شوند، می‌توانند مبتنی بر ارسال رشته بیت یا مبتنی بر ارسال رشته بایت باشند.

لایه دوم از مدل TCP/IP : لایه شبکه

- بسته‌های IP بسته‌های اطلاعاتی در این لایه
- هدایت بسته‌های IP روی شبکه از مبدأ تا مقصد که این عمل از نوع بدون اتصال می‌باشد
- ویژگی ارسال چندپخشی یعنی ارسال یک یا چند بسته اطلاعاتی به چندین مقصد گوناگون در قالب یک گروه سازماندهی‌شده
- پروتکلهائی که در این لایه استفاده می‌شوند عبارتند از:

IP , IGMP , BOOTP , ARP , RARP , RIP , ICMP و . .

لایه سوم از مدل TCP/IP : لایه انتقال

برقراری ارتباط از طـریق یـک سرویس اتصال‌گرا و مطمئـن با ماشینهای انتهایی یا میزبان.

ارسال و یا دریافت داده‌های تحویلی به این لایه توسط برنامه‌های کاربردی و از طریق توابع سیستمی

لایه چهارم از مدل TCP/IP : لایه کاربرد

خدماتی که در این لایه صورت می‌گیرد در قالب پروتکلهای استاندارد زیر به کاربر ارائه می‌شود :

شبیه‌سازی ترمینال

انتقال فایل یا FTP

مدیریت پست الکترونیکی

خدمات انتقال صفحات ابرمتنی

به نام خدا

طراحی و پیاده سازی
زیر ساخت
شبکه های کامپیوتری

مدرس: مهندس مليحه اميني

آشنايي با مفهوم Host در پروتكل TCP/IP

تعريف: به هر سيستم در شبكه كه از TCP/IP براي ارتباط استفاده كند اصطلاحاً يك TCP/IP Host يا ميزبان TCP/IP مي گوييم.

هر Hostدر TCP/IP داراي دو مشخصه اصلي و بارز است. بعبارت ديگر هر Host را مي توان با دو خصوصيت از بقيه Hostها تفكيك كرد. اين دو مشخصه عبارتند از:

الف- نام (Host Name)

ب- آدرس (Host Address =IP Address)

الف- نام (Host Name)

تذکر: برای سهولت بیشتر کاربران، برای اکثر میزبانهای مهم یک یا چند نام انتخاب می شود.

بدیهی است که این نامها باید از قوانینی تبعیت کرده و ضمنا مورد تایید مراکز ثبت اسامی نیز قرار بگیرند به زبان دیگر باید اسم را ثبت یا (Register) کرد.

الف- نام (Host Name) ...

دو قالب برای نامگذاری وجود دارد:

قالب اول: هر یک از اسامی زیر بعنوان یک Host Nameمی تواند در پروتکل TCP/IPاستفاده شود.

reza server22 Client80 PC1

Moon C1

قالب دوم:

www.yahoo.com

www.sanjesh.ir

mail.yahoo.com

ftp.dlink.com

www.dci.ir

پرسش۱: تفاوت بین قالب اول و دوم در چیست؟

معمولا اسامی قالب اول در محدوده داخلی شبکه ها استفاده شده، نیازی به ثبت ندارند اما اسامی قالب دوم عمدتا ثبت شده و در این صورت چه در محدوده داخلی و چه افراد خارج از شبکه داخلی می توانند از آن برای مراجعه به Host استفاده کنند.

پرسش۲: يك اسم در قالب دوم معمولا از چه قسمت هايي تشكيل مي شود.

الف- نام سرویسی که Host ارائه می دهد یا نقشی که Host بازی می کند.

www= Web Server mail= Mail server

ftp= FTP Server

ب- نام شرکت، سازمان، مجموعه یا شخصی که Host بدان تعلق دارد. (Computer Name)

مثال:

Yahoo, google, irib, sun, microsoft ,…

ج-حوزه فعالیت میزبان (Activities)

com, net, org, gov, edu, ac, info, tv,….

د- وابستگی منطقه ای و محلی اعم از فرهنگی؛ اجتماعی و .... یا زبان استفاده شده در سایت.(locality)

Ir = iran tr= turkey uk= United Kingdom

,…

برای دیدن لیست کاملی از کدهای دو حرفی مربوط به کشورهای مختلف در google عبارت زیر را جستجو کنید: Country codes یا مستقیما به سایت www.iana.org مراجعه کنید.

نکته ۱: همانطور که گفته شد اسامی اعم از قالب اول یا دوم در ابتدای کار بوسیله TCP/IP به آدرس تبدیل می شوند.

نکته ۲: به اسامی که در قالب دوم قرار دارند اصطلاحا FQDN گفته می شود.

Fully Qualified Domain Name

نکته ۳: در یک FQDN چنانچه بخش ابتدایی سمت چپ را که (بیانگر نام سرویس است) کنار بگذاریم، به مجموع بقیه قسمت ها Domain گفته می شود که شامل نام شرکت، حوزه فعالیت و کشور می شود.

بنابراین:

FQDN بطور کلی از دو بخش تشکیل شده:

FQDN= Service Name + Domain Name

www + microsoft .com

ftp + dlink.com

به مجموعه های یک Domain اصطلاحاً Sub Domain می گویند.

در عمل معمولا از Sub Domain برای نشان دادن شرکت ها، زیرگروه ها یا ساختارهای فرعی در یک مجموعه‌ی بزرگ استفاده میشود.

مثال:

فرض کنید یک شرکت بزرگ کامپیوتری علاوه بر شرکت اصلی، از سه شرکت زیر مجموعه برای فعالیتهای سخت افزار، نرم افزار و شبکه استفاده می کند.

برای شرکت اصلی، یک Domain بنام main.net را در نظر گرفته آن را ثبت می کنیم. حال با توجه به گستردگی فعالیتهای شرکت بزرگ و طبیعتاً شرکت های زیر مجموعه نیز یک Domain در نظر گردد:

برای شرکت سخت افزار: hardwar.main.net

برای شرکت نرم افزار: software.main.net

برای شرکت شبکه: network.main.net

هر یک از Domainهای فوق را اصطلاحاً یک Sub Domain از main.net می نامند.

چنانچه شرکت اصلی و بخش های تابعه، هر یک برای خود Web Server داشته باشند در آن صورت دارای اسامی زیر خواهند بود:

وب سرور شرکت اصلی www.main.net

وب سرور شرکت سخت افزار www.hardware.main.net

وب سرور شرکت نرم افزار www.software.main.net

وب سرور شرکت شبکه www.network.main.net


Web server
mail server
Computer name
Activity
www.mail.yahoo.com
Activity
www.irib.tv.ir
Web server
Computer name
Locality

در كامپيوترهايي كه از سيستم عاملهاي مايكروسافت بهره برده و در ضمن پروتكل TCP/IP روي آنها فعال مي شود، نكات زير داراي اهميت است:

✓Computer Name كه به NetBIOS Name نيز معروف است، يك اسم ۱۵ كاركتري منحصربه فرد است كه زمان نصب OS به آن داده ميشود.

✓در سيستم عامل XP براي تغيير NetBIOS از System Properties استفاده مي شود.

✓TCP/IP Name كه همان Host Name در پروتكل TCP/IP است به Full Computer Name معروف است و ممكن است قالب اول يا دوم باشد. بصورت پيش فرض در كامپيوترهايي كه عضو Work group باشند TCP/IP دقيقا برابر با NetBIOS است.

✓اگر رايانه به عضويت Domain در Active Directory در آيد آنگاه TCP/IP Name به صورت زير است:

TCP/IP Name = NetBIOS Name + Active Directory Domain Name

يعني TCP/IP Name در قالب دوم مي شود.

ب- Host Address = IP Address

هر Hostدر پروتکل TCP/IPباید حداقل یک آدرس منحصر به فرد داشته باشد که به آن IP Addressمی گویند.

منحصر به فرد بودن زمانی مهم است که شبکه ها با یکدیگر در ارتباط باشند و گرنه زمانیکه هیچگونه ارتباطی (با روتر) بین شبکه ها برقرار نیست چه اهمیتی دارد که آدرس های مورد استفاده در یک شبکه با دیگر شبکه ها تکراری باشد.

تعریف IP Address

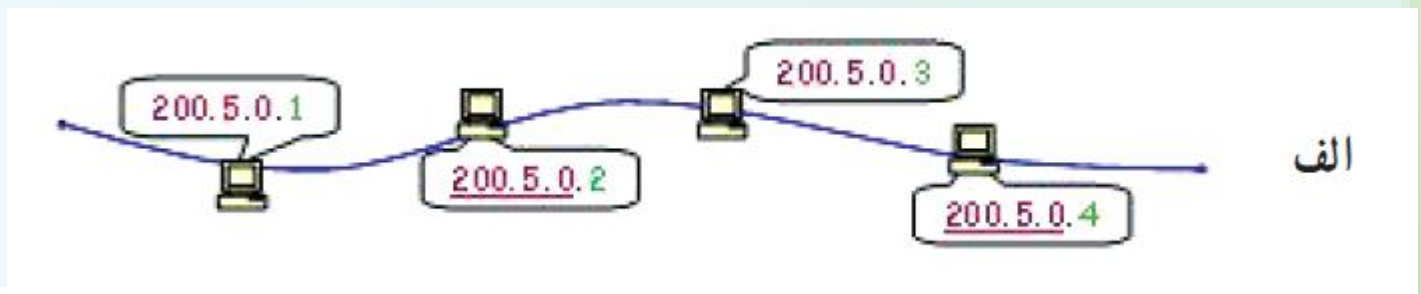
یک عدد ۴ بایتی (۳۲ بیتی) بوده که به فرم w.x.y.z تنظیم می شود. (0<w.x.y.z<255)

به نکات زیر همراه با شکلهای مربوطه دقت کنید:

- هر آدرس از دو قسمت تشکیل شده: یک قسمت در سمت چپ که بین تمام سیستم های بکار رفته در هر شبکه مشترک است و یک قسمت در سمت راست که برای هر سیستم منحصر بفرد است:

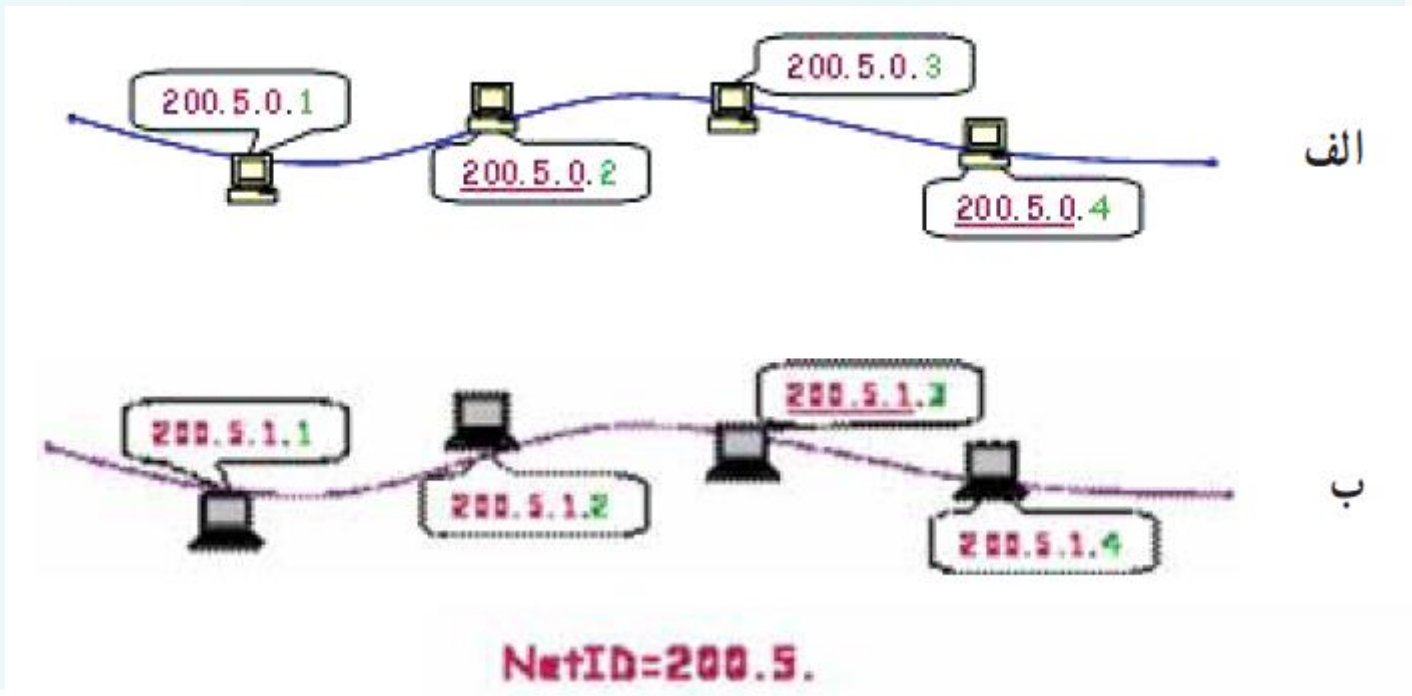
a-Network ID or Net ID

b- Host ID or Node ID



تعریف IP Address ...

از مقایسه شکل ها با یکدیگر در می یابیم که شبکه های مختلف هر کدام NetID های مختلفی دارند و تکراری نیست.



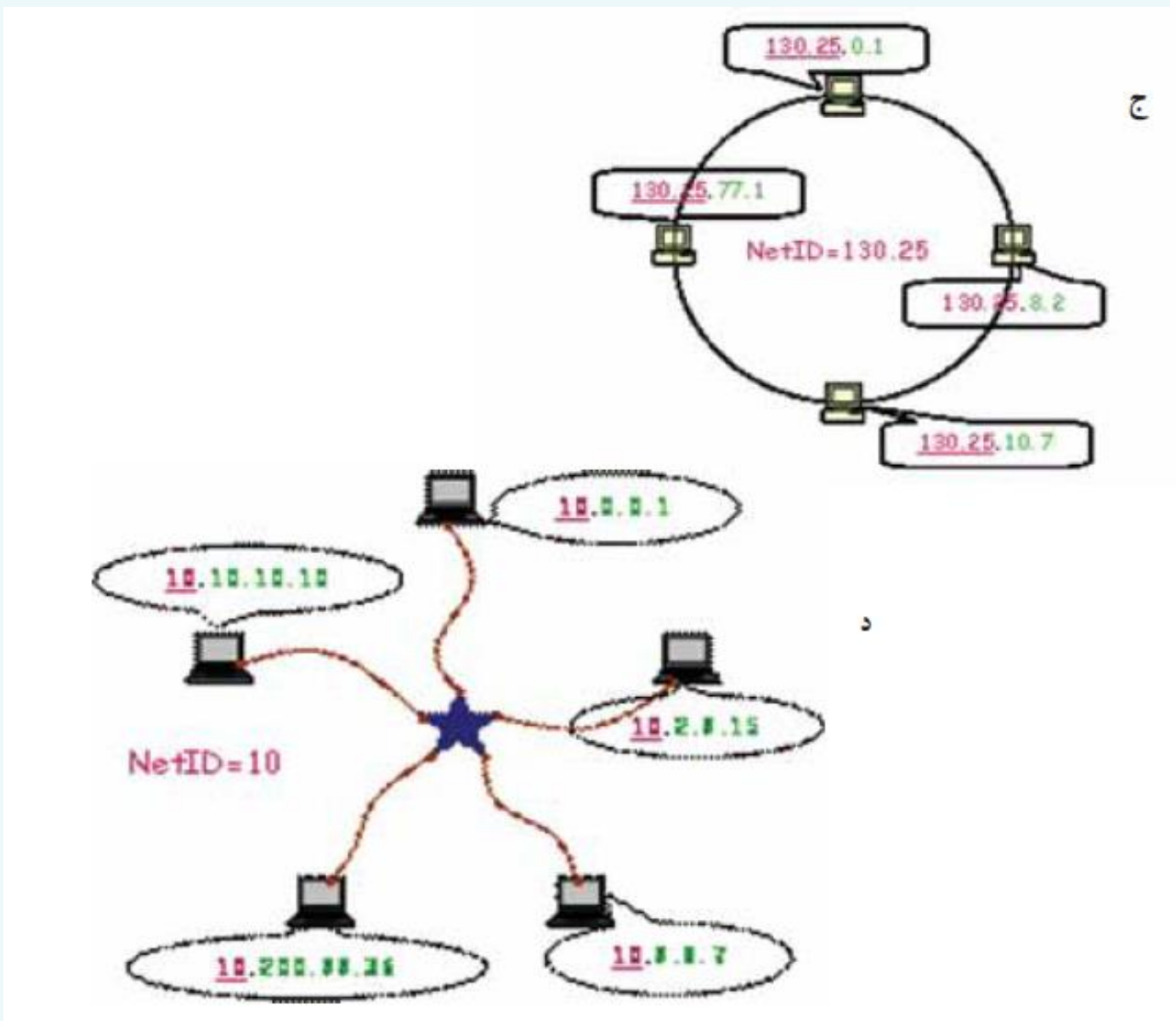
تعریف IP Address ...

- NetID ممکن است ۳ بایت (شکلهای الف و ب) یا ۲ بایت (شکل ۳) یا ۱ بایت (شکل ۴) باشد.

بدیهی است که هر چه تعداد بایتهای NetID بیشتر باشد شبکه های بیشتری را می توان شماره گذاری کرد اما از آن طرف تعداد Hostهای موجود در شبکه محدودتر می شود.

بسته به اینکه تعداد بایتهای NetIDچند رقم باشد ۳ کلاس متفاوت IP Addressپدید می آید:

Net ID = 1 Byte (8bits) ➔ Class A
Net ID = 2 Byte (16bits) ➔ Class B
Net ID = 3 Byte (24bits) ➔ Class C


130.25.0.1
ج
130.25.77.1
NetID=130.25
130.25.8.2
130.25.10.7
10.0.0.1
10.10.10.10
10.2.0.15
NetID=10
10.200.88.26
10.0.0.7
د

با مشاهده IP Address چگونه متوجه مي شويم در چه كلاسي است؟ (يعني NetIDو HostIDكدام است؟)

جدول زیر نشانگر نوع کلاسهاست:

W	Class
1 – 126	A
128 – 191	B
192 – 223	C
224 _ 239	D

یعنی از روی رقم اول سمت چپ (W) می توانیم بفهمیم که یک آدرس در چه کلاسی است.

با مشاهده IP Address چگونه متوجه مي شويم در چه كلاسي است؟ (يعني NetIDو HostIDكدام است؟) ...

چند سوال برای روشن تر شدن کلاسها:

۱. آیا W نمی تواند با صفر شروع شود؟ خیر IP Address نمی تواند با عدد صفر شروع شود.
۲. عدد ۱۲۷ کجاست؟ هر آدرسی که بصورت 127.x.y.z باشد اصطلاحاً Loop Back خوانده می شود.
۳. محدوده ۲۴۰ تا ۲۵۵ به چه دردی می خورد؟ در رقم اول هیچگاه تا این لحظه مورد استفاده عملیاتی قرار نگرفته و صرفا جنبه آزمایشی داشته است لذا برای آن کاربردی تعریف نشده است.

نکته:

آدرس های موجود در کلاس A,B,C برای Unicast و کلاس D برای Multicast استفاده می شود.

توضیحات بیان شده در مورد آدرس ها در جدول زیر خلاصه شده است:

Class	Usage	W	Net ID	Host(Node) ID
A	Unicast	1 – 126	1 Bytes (8 bits)	3 Bytes
B	Unicast	128 – 191	2 Bytes (16 bits)	2 Bytes
C	Unicast	192 – 223	3 Bytes (24 bits)	1 Byte
D	Multicast	224 – 239		

قوانين آدرس دهي

۱- قانون اول: در یک شبکه مشخص، هر Hostباید حداقل یک آدرس منحصر به فرد در یکی از کلاس های A,B,Cرا داشته باشد. ضمنا هر شبکه دارای Net IDجداگانه ای از سایر شبکه های دیگر است.

۲- قانون دوم: در یک شبکه مشخص برای آنکه کلیه Hostها بتوانند مستقیماً و بدون واسطه با یکدیگر ارتباط داشته باشند، باید دارای Net IDیکسان باشند.

۳- قانون سوم: Host IDنمی تواند همگی با هم صفر باشد یا همگی باهم ۲۵۵ باشد.

٤- Net IDنمی تواند همگی با هم صفر باشد یا همگی باهم ۲۵۵ باشد.

Subnet mask

- Subnet mask روشی برای تشخیص کلاس آدرس IPمیباشد.در واقع نشان دهنده تعداد بیتهای Net ID میباشد.

Class A: 255.0.0.0

Class B: 255.255.0.0

Class C: 255.255.255.0

مسیریابها برای تشخیص Net ID از روی یک آدرس IP، آدرس IP و Subnet maskرا با هم AND میکنند.

مثال:

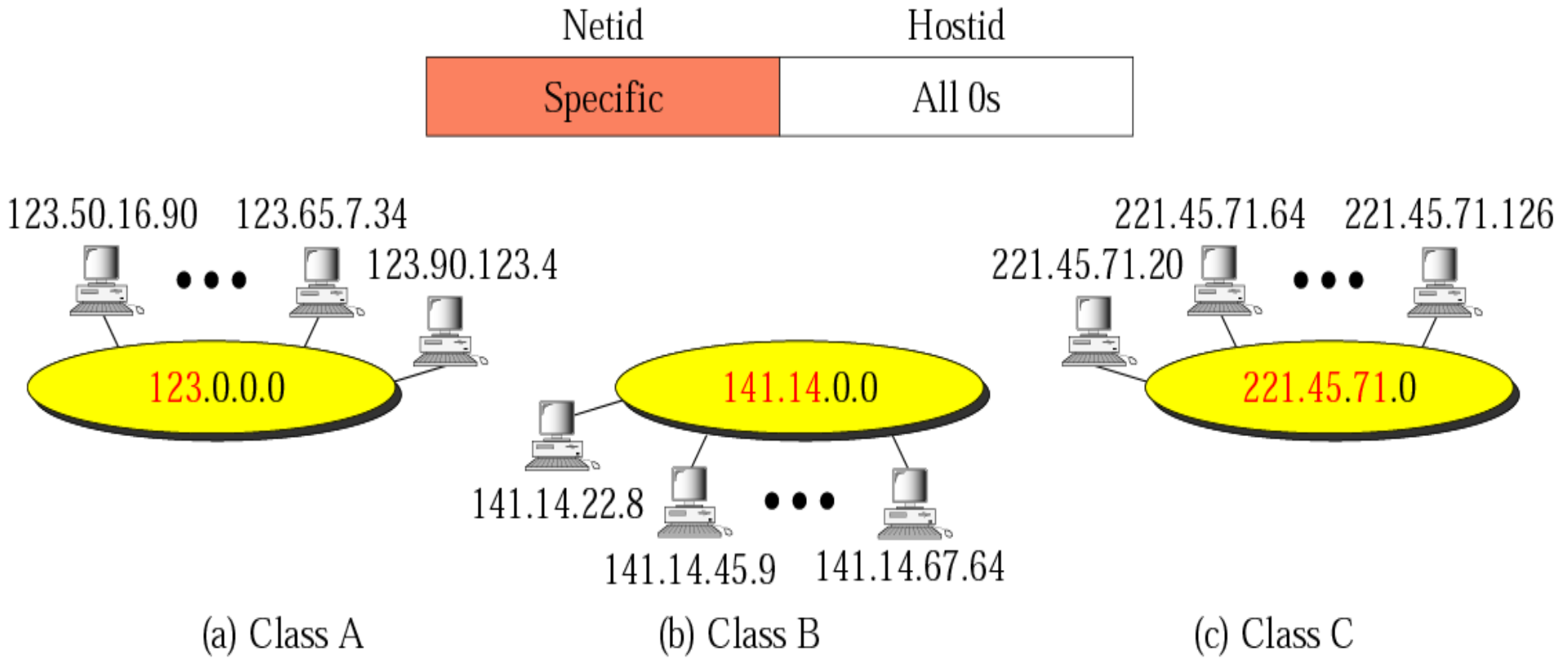
IP:131.57.17.9

Subnet mask: 255.255.0.0

➔ Net id: 131.57.0.0

Figure 4-13

Network addresses



مسیریابي بين ناحيه‌اي بدون كلاس

CIDR (Classless Inter-Domain Routing)

اخیرا بدلیل افزایش کاربران اینترنت پروتکل IPبا کمبود فضای آدرس مواجه شده است بهمین دلیل دیگر استفاده از کلاسهای معمول برای آدرسدهی این همه میزبان اینترنت کفایت نمیکند بنابراین از روش مسیریابی بدون کلاس استفاده میشود.محدوده host کلاس Aخیلی بزرگ است در حالیکه این محدوده برای کلاس c کم است.بانبراین استفاده از کلاسهای استاندارد در اینترنت مناسب نیست و باید کلاسها را تغییر داد،اینکار با استفاده از مکانیزمی بنام subnettingانجام میشود.

مسيريابي بين ناحيه‌اي بدون كلاس

CIDR (Classless Inter-Domain Routing)

مزايا:

- استفاده مناسب از فضاي آدرس‌هاي IP،
- Supernetting به اين معني است كه يک سطر جدول مسيريابي بلوكي از آدرس‌هاي طبقه بندي شده پشت سر هم را پوشش مي‌دهد.

معايب:

- جدول مسيريابي بايد توانايي نگهداري معرفي كننده شبكه با طول متغير را داشته باشند،
- پيدا كردن حداكثر تطابق پيشوند در جدول مسيريابي.

Subnetting

- در مسیریابی بر اساس آدرسهای بدون کلاس دیگر کلاسهای استاندارد استفاده نمیشوند بلکه یک محدوده آدرس IP استاندارد میتواند شکسته شده ودر اختیار چندین شبکه کوچکتر قرار گیرد.
- تبدیل یک Net ID به چندین Net ID را SUBNETTINGگویند.برای انجام اینکار بایستی بنا بر شرایط تعدادی از بیتهای Host ID را گرفته و به Net ID بیافزاییم.روش انجام کار استفاده از فرمول مقابل انجام میشود : تعداد subnetها $\geq 2^n$
- nتعداد بیتهایی است که قرض میگیریم. حالتهای مختلفی را که با این n بیت بدست می آید را subnet numberمینامیم.بیتهای باقیمانده host id برای هر زیر شبکه بحساب می آیند.
- Subnet maskتمام زیر شبکه ها با هم برابر است ولی subnet number آنها متفاوت است.

Figure 5-1

A network with two levels of hierarchy (not subnetted)

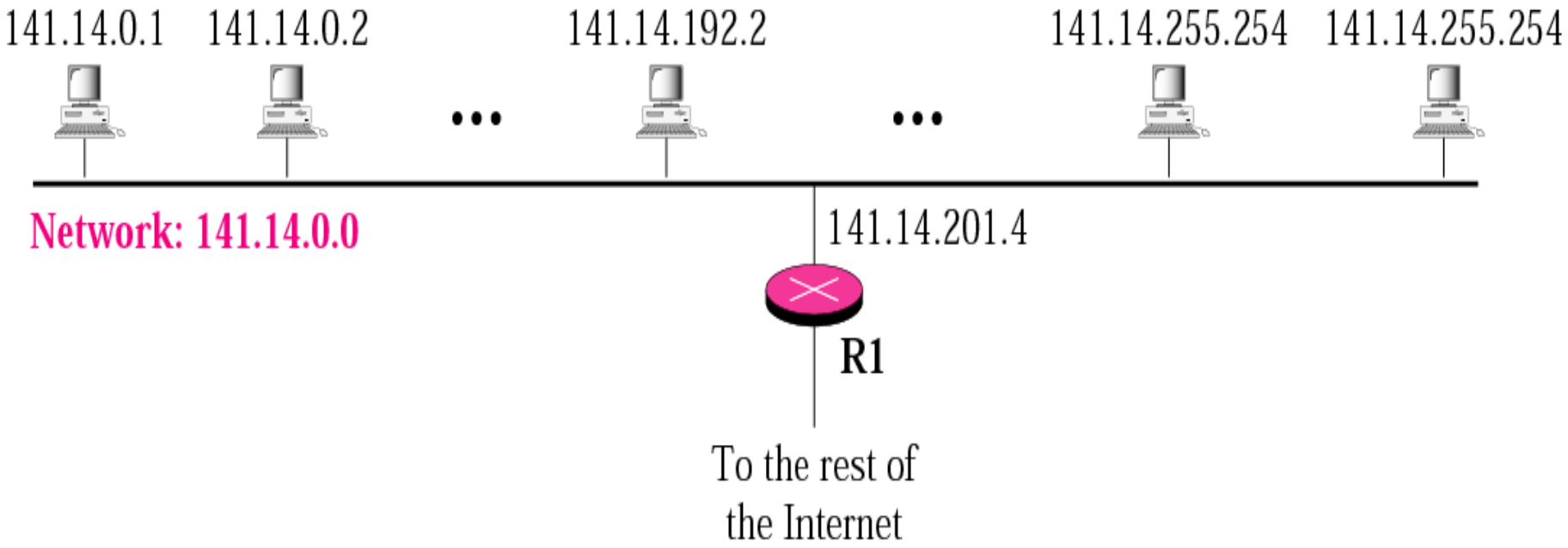
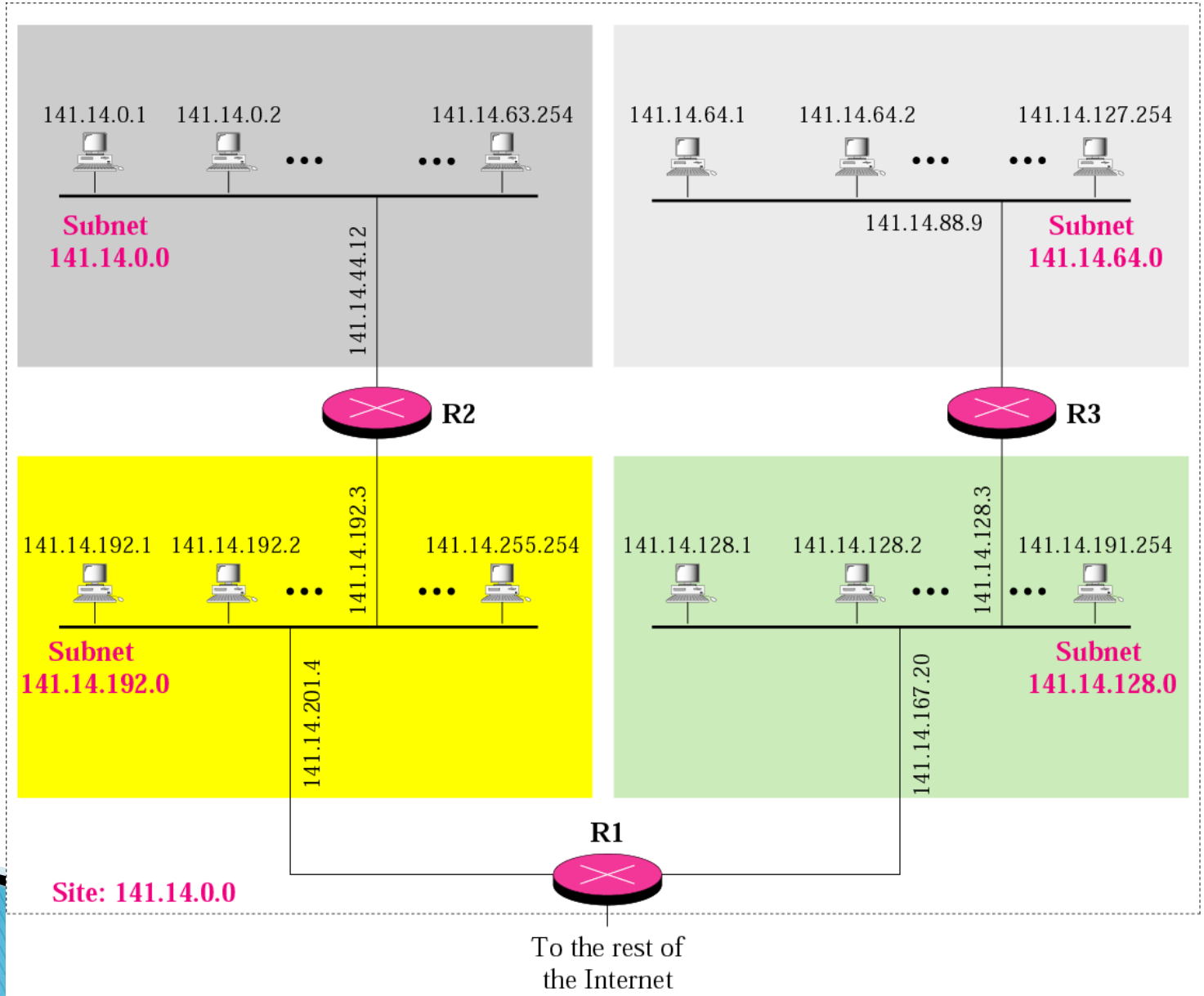


Figure 5-2

A network with three levels of hierarchy (subnetted)



مثال

- میخواهیم یک آدرس کلاس cبفرم 192.168.5.0 را تبدیل به ۴ تا subnetکنیم.محدوده آدرس هر یک از این subnetها را بدست آورید.

جواب:چون ۴ تا زیر شبکه داریم n=2یعنی دو بیت کفایت میکند .

192.168.5.00000000

چهار حالت مختلف میتوان با این ۲ بیت داشت یعنی :

00,01,10,11

که نشان دهند ۴ شبکه مختلف است.

مثال ...

Subnet number

اولین آدرس مجاز

Subnet1:192.168.5.00------:192.168.5.0/26 : from 192.168.5.1 to 192.168.5.62

آخرین آدرس مجاز

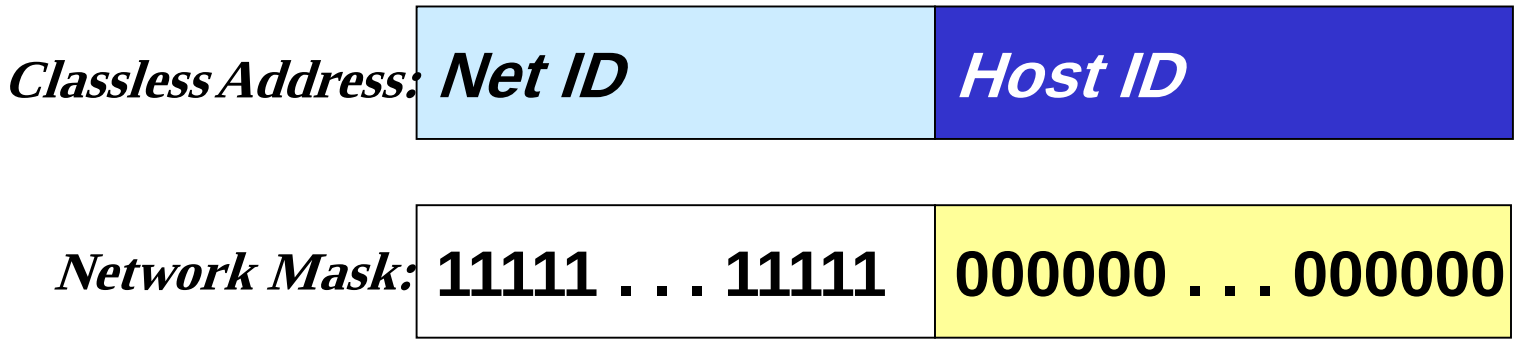
Subnet2:192.168.5.01------:192.168.5.64/26: from 192.168.5.65 to 192.168.5.126

Subnet3:192.168.5.10------:192.168.5.128/26: from 192.168.5.129 to 192.168.5.190

Subnet4:192.168.5.11------:192.168.5.192/26: from 192.168.5.193 to 192.168.5.255

چون ۲۶بیت برای Net_id استفاده شده و کلاس دیگر استاندارد نیست تعداد بیتهای سابنت باید همراه آدرس ذکر شود.

مسیریابي بین ناحیه‌اي بدون کلاس ...
CIDR (Classless Inter-Domain Routing)



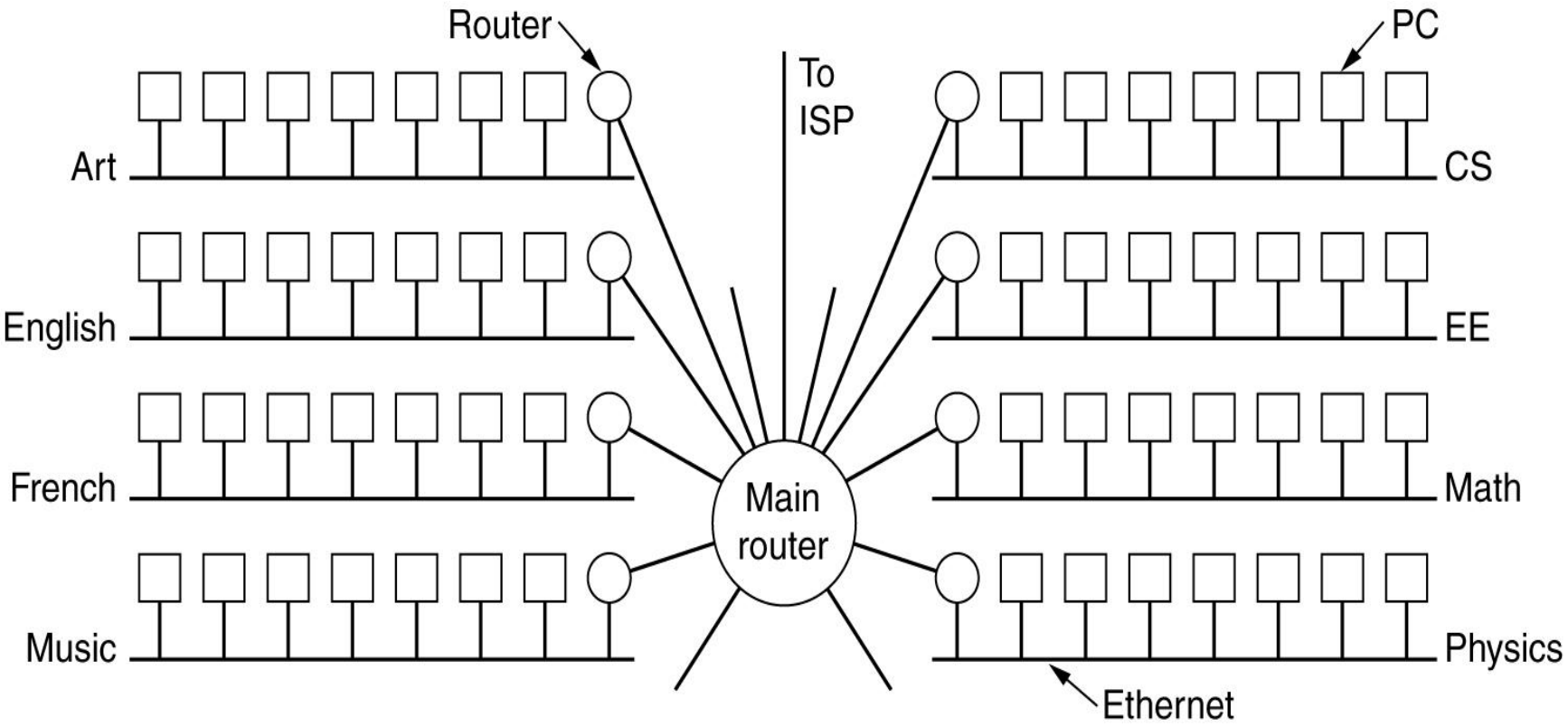
Route Prefix / Prefix Length

w.x.y.z/m

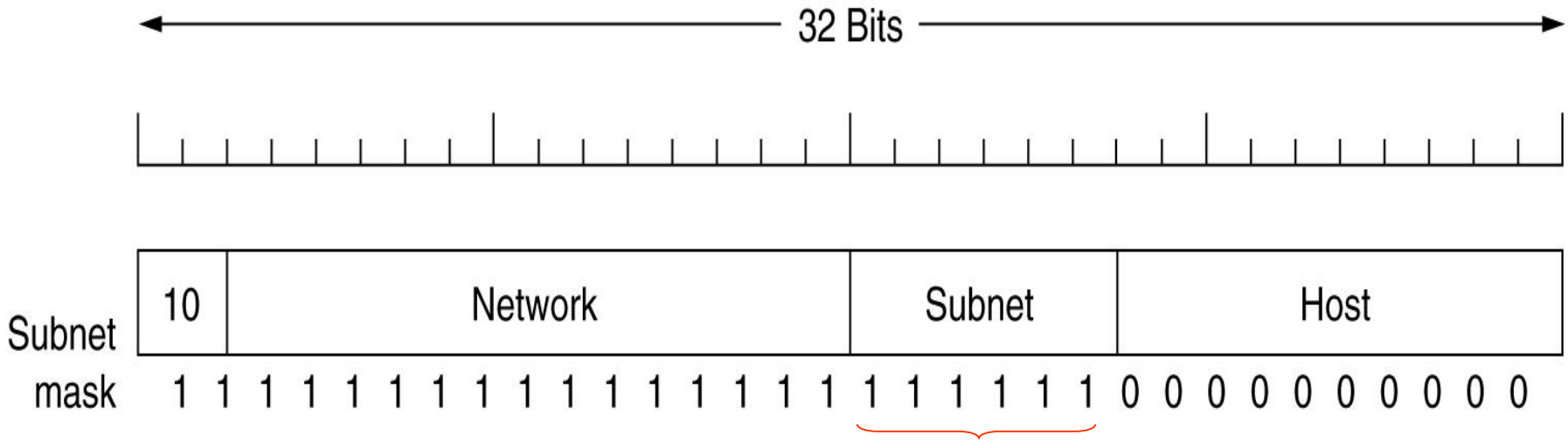
Example: **205.100.0.0/22**

Subnets

یک شبکه بزرگ شامل lanهايي براي قسمتهاي مختلف



Subnets (2)



با ۶ بیت میتوان ۶۴حالت مختلف ایجاد نمود یعنی به ۶۴ زیرشبکه تقسیم کرد

A class B network subnetted into 64 subnets.

مسيريابي بين ناحيه‌اي بدون كلاس ...
CIDR (Classless Inter-Domain Routing)

نمونه ای دیگر از اختصاص آدرس IPبه چهار دانشگاه

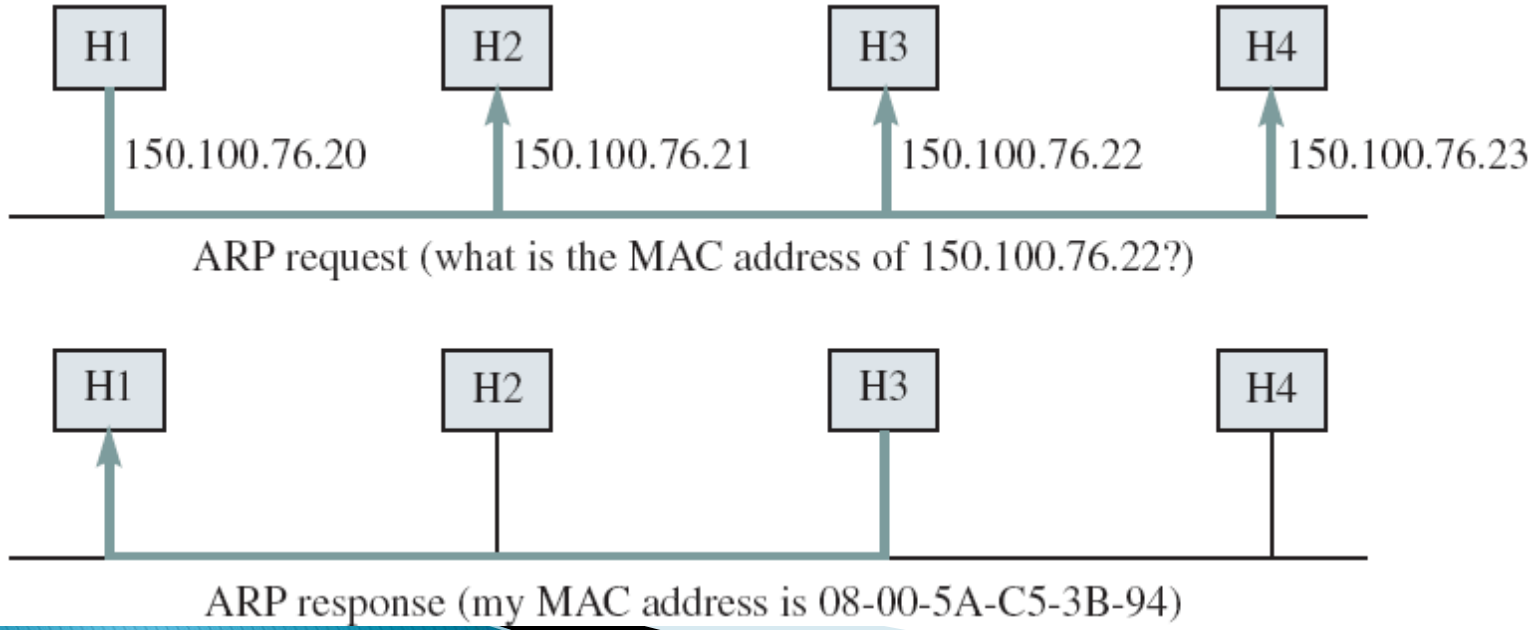
نام دانشگاه	اولین آدرس شبکه	آخرین آدرس شبکه	تعداد host هاي شبکه	نحوه نوشتن آدرس
Cambridge	194.24.0.0	194.24.7.255	2048	194.24.0.0/21
Edinburgh	194.24.8.0	194.24.11.255	1024	194.24.8.0/22
(Available)	194.24.12.0	194.24.15.255	1024	194.24.12/22
Oxford	194.24.16.0	194.24.31.255	4096	194.24.16.0/20

پروتکل حل آدرس
(Address Resolution Protocol)

به پروتکلی که نگاشت بین آدرس‌های IP و آدرس‌های فیزیکی (آدرس‌های واسط شبکه) را انجام می‌دهد پروتکل حل آدرس (ARP)گفته می‌شود.دلیل استفاده از این روش اینست که وقتی کامپیوتری میخواهد بسته ای را برای کامپیوتر دیگری در همان شبکه ارسال نماید باید بسته را به لایه پایینی یعنی لایه Data linkتحویل دهد و از آنجاییکه این لایه آدرسهای IPرا نمی فهمد و فقط آدرس های فیزیکی رامیفهمد باید آدرس فیزیکی کامپیوتر مقصد را بدست آورد.

پروتکل حل آدرس
(Address Resolution Protocol)

در شکل مثالی از پروتکل ARP در حالتی که تکنولوژی شبکه لایه زیرین، شبکه اترنت می‌باشد نشان داده شده است. در این مثال کامپیوترH1 می‌خواهد آدرس MAC کامپیوتر H3 را با فرض در اختیار داشتن آدرس ipآن بدست آورد، برای این منظور پیام درخواستی در شبکه پخش کرده و از H3 می‌خواهد که آدرس MAC خود را اعلام کند، H3با دریافت این پیام در پاسخ آدرس MAC خود را به H1 اطلاع می‌دهد.



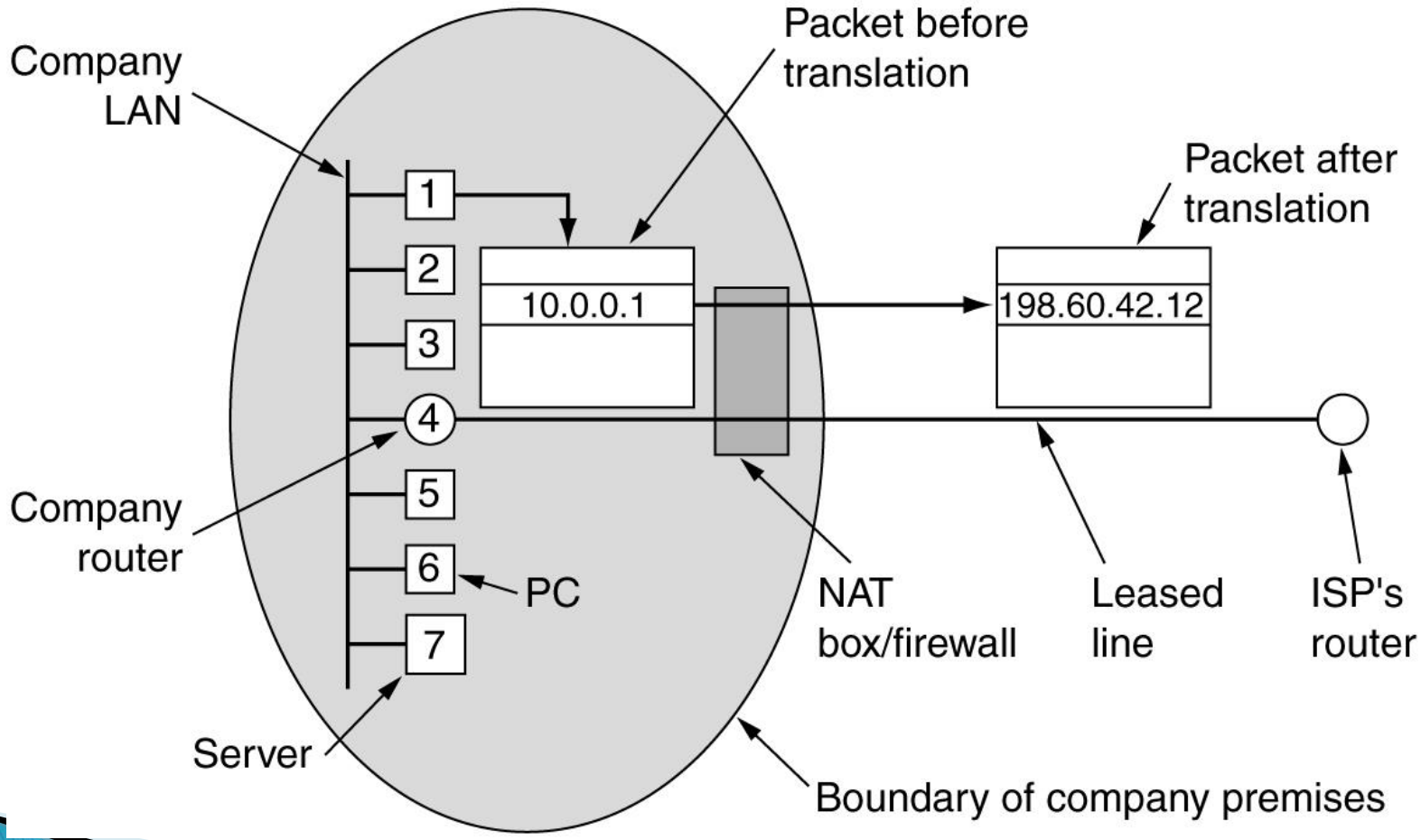
پروتکل معکوس حل آدرس
(Reverse Address Resolution Protocol)

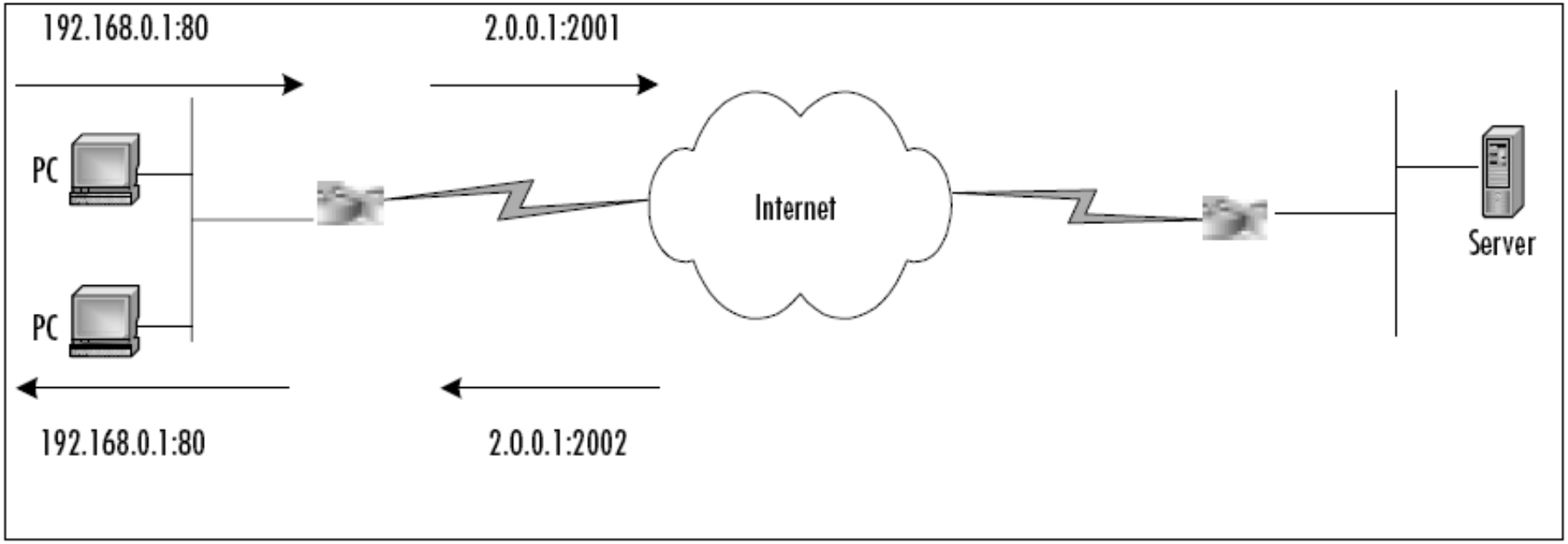
پروتکل معکوس حل آدرس یا RARP، پروتکلی است که از روی آدرس فیزیکی، آدرس IP یک کامپیوتر را بدست می‌آورد.یعنی عکس ARPعمل میکند.بعلت نواقص این پروتکل بعدها پروتکلهای BOOTPوDHCPارائه شدند که این آخری کاربرد زیادی دارد چون بصورت اتوماتیک به کامپیوترهای شبکه آدرس IP تخصیص میدهد.

Network Address Translation(NAT)

- آدرسهای IPکمیاب هستند.در مورد کاربران خانگی آدرسهای IP موقتا اختصاص داده میشود و بعد از قطع ارتباط پس گرفته میشود ولی در مورد کاربران ثابت مثل ادارات و یا کافی نتها و یا کاربران ADSL نمیتوان اینکار را کرد و باید به آنها IP ثابت داد ولی از آنجا که ممکن است IP های یک ISPبه تعداد کاربران نباشد راه حل دیگری ارائه شد که NAT نام دارد. در این ایده مثلا به کافی نت فقط یک آدرس IP معتبرجهانی داده میشود و تمامی کامپیوترها هر کدام یک آدرس IP دارند ولی نه از نوع معتبر و جهانی بلکه از نوع Invalid. وقتی یکی از این کامپیوترها میخواهد بسته ای را به خارج شبکه (مثلا اینترنت) ارسال کند باید قبل از خروج بسته ترجمه آدرس انجام گیرد و آدرس IP معتبر جایگزین آدرس نامعتبر میشود،البته این اتفاق فقط زمانی می افتد که مقصد بسته خارج از این شبکه باشد.

Network Address Translation(NAT)




192.168.0.1:80
2.0.0.1:2001
PC
PC
Internet
Server
192.168.0.1:80
2.0.0.1:2002

خصوصي يا عمومي

A computer on the Internet is identified by its IP address.

In order to avoid address conflicts, IP addresses are publicly registered with the Network Information Centre (NIC). Computers on private TCP/IP LANs however do not need public IP addresses, since they do not need to be accessed by the public. For this reason, the NIC has reserved certain addresses that will never be registered publicly.

These are known as private IP addresses, and are found in the following ranges:

محدوده آدرسهاي خصوصي

IANA-reserved private IPv4 network ranges			
	Start	**End**	**No. of addresses**
24-bit Block (/8 prefix, 1 × A)	10.0.0.0	10.255.255.255	16 777 216
20-bit Block (/12 prefix, 16 × B)	172.16.0.0	172.31.255.255	1 048 576
16-bit Block (/16 prefix, 256 × C)	192.168.0.0	192.168.255.255	65 536

Network Address Translation(NAT)

محدوده آدرسهای خصوصی(private Addresses)

- این آدرسها برای استفاده در داخل شبکه ها کنار گذاشته شده اند:
- 10.0.0.0 to 10.255.255.255/8
- 172.16.0.0 to 172.31.255.255/12
- 192.168.0.0 to 192.168.255.255/16

سایر آدرسها آدرسهای عمومی هستند که در اینترنت استفاده میشوند. داخل شبکه محلی از آدرسهای خصوصی استفاده میشود.

- اگر بسته ای وارد شد جعبه NAT از کجا بفهمد برای کدام ماشین است: از روی شماره پورت در هدر لایه Transport .جعبه NATتضمین میکند که هیچ دو ماشینی شماره پورت یکسانی نداشته باشند.

پروتکلICMP (پروتکل پیام کنترل اینترنت)

- ICMPمخفف Internet Control Message Protocol است و در RFC792 جزئیات مربوط به آن ارائه شده است.
- این پروتکل بخشی از پروتکل های لایه اینترنت را تشکیل می دهد و از دیتاگرام IP برای ارسال پیغام های خود استفاده می کند.
- وظایف ICMP:
  - کنترل جریان.
  - گزارش خطا.
  - ارائه عملکرد های اطلاعاتی به مجموعه پروتکل های TCP/IP.
- کنترل جریان:
  - وقتی دیتاگرام های IP با سرعت بالا جهت پردازش به ایستگاه یا Host مورد نظر می رسند، ایستگاه مقصد ویا Gateway میانی پیغام ICMP Source Quench را به فرستنده ارسال می کند و از این طریق از ارسال دیتاگرام های متوالی توسط فرستنده جلوگیری به عمل می آورد.

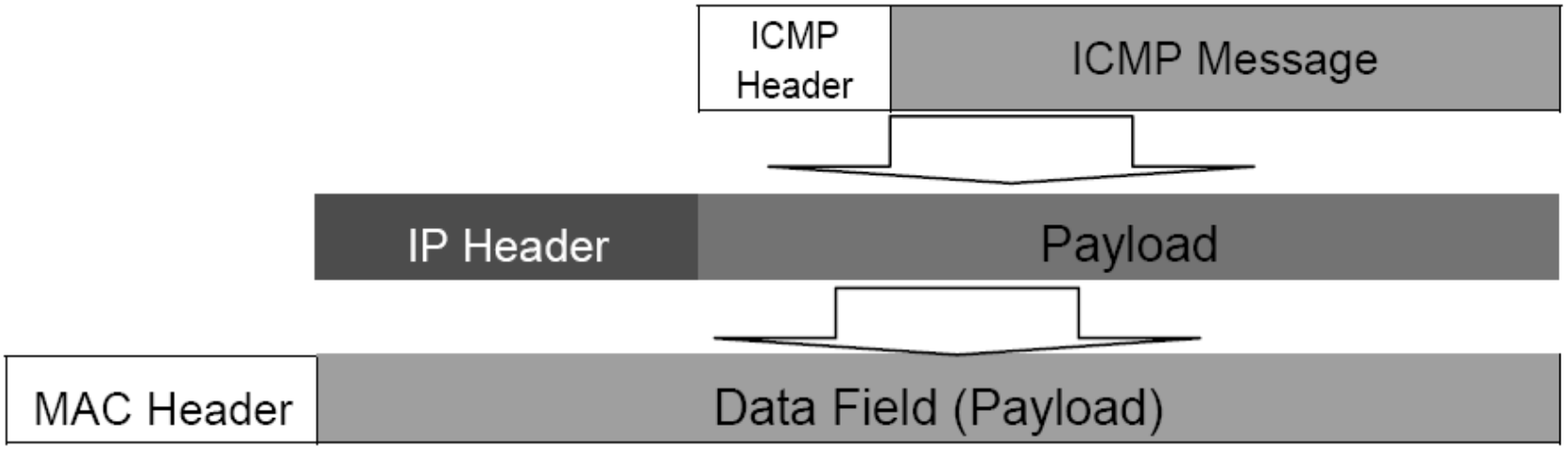
پروتکل ICMP (پروتکل پیام کنترل اینترنت) ...

- تشخیص عدم دسترسی به مقصد
  - زمانی که امکان دسترسی به ایستگاه مقصد در شبکه موجود نباشد، سیستم تشخیص دهنده آن پیغام مقصد در دسترس نمی باشد را به فرستنده ارسال می کند. اگر شبکه مقصد مورد نظر در دسترس نباشد، Gateway میانی این پیغام را ارسال می کند و اگر پورت ایستگاه مقصد در دسترس نباشد، خود ایستگاه مقصد پیغام را ارسال می کند.
- تغییر مسیر
  - Gateway پیغام تغییر مسیر (ICMP Redirect) را به فرستنده به منظور تغییر مسیر ارسال، می فرستند.
- بررسی ایستگاه خارجی
  - برای بررسی فعالیت پروتکل لایه اینترنت ایستگاه خارجی می توان پیغام ICMP Echo را ارسال کرد.
  - وقتی یک سیستم پیغام Echo را دریافت می کند، داده موجود در پیغام را به فرستنده باز می گرداند.
  - مثال: Ping.

پروتکل ICMP (پروتکل پیام کنترل اینترنت) ...

پروتکل ICMP پروتکل مدیریتی لایه IP می‌باشد که پیام‌های خود را توسط بسته‌های IP مبادله می‌کند. برنامه‌های کاربردی ping، traceroute از جمله کاربردهای مدیریتی هستند که از پروتکل ICMP استفاده می‌کنند.مثلا در PING چند بسته Echo ارسال میشود و اگر ماشین مقصد فعال باشد با بسته های Echo reply پاسخ میدهد.

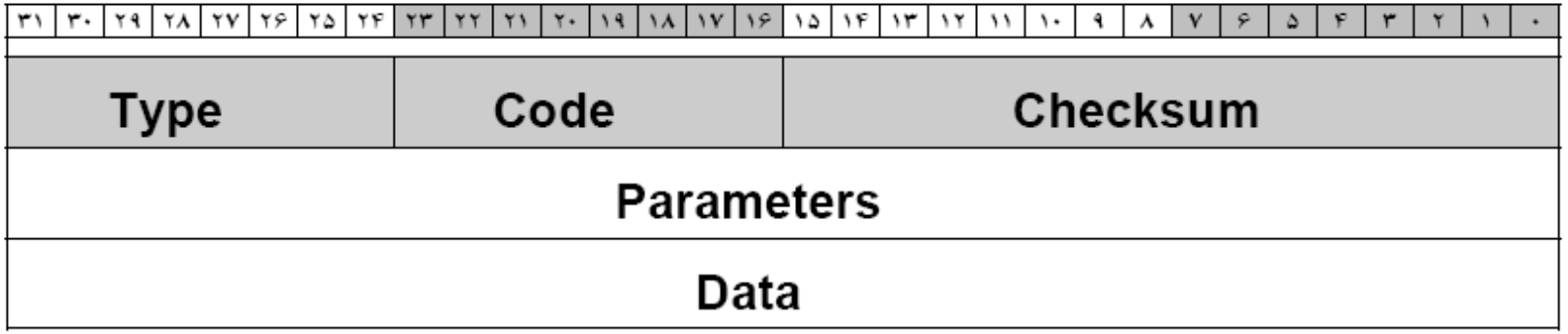
پروتکل ICMP (پروتکل پیام کنترل اینترنت) ...



چگونگی قرار گرفتن یک پیام ICMP درون یک بستهٔ IP

با توجه به آنکه پیام ICMP خود درون یک بسته IP جاسازی می‌شود بنابراین فیلد Protocol در سرآیند بستهٔ IP باید با شمارهٔ مشخصهٔ پروتکل ICMP (یعنی ۱) تنظیم شود.

شکل کلّی و قالب پیام ICMP در زیر مشخص شده است:



- فیلد **Type** : در این فیلد عددی قرار می‌گیرد که بیانگر نوع پیام می‌باشد و ساختار فیلدهای Parameters و Data بسته به عددی که در این فیلد قرار می‌گیرد متفاوت خواهد بود.
- فیلد **Code** : گاهی خود نوع پیام به چند زیر نوع دیگر تقسیم می‌شود که کد زیر نوع در این فیلد قرار می‌گیرد.
- فیلد **Checksum** : محتوای این فیلد برای سنجش اعتبار و سلامت بستهٔ ICMP مورد استفاده قرار می‌گیرد. تمامی بستهٔ ICMP بصورت دوبایت دوبایت جمع شده و نهایتاً از مکمل ۱ حاصل جمع ، عددی ۱۶ بیتی بدست می‌آید که درون این فیلد قرار می‌گیرد.

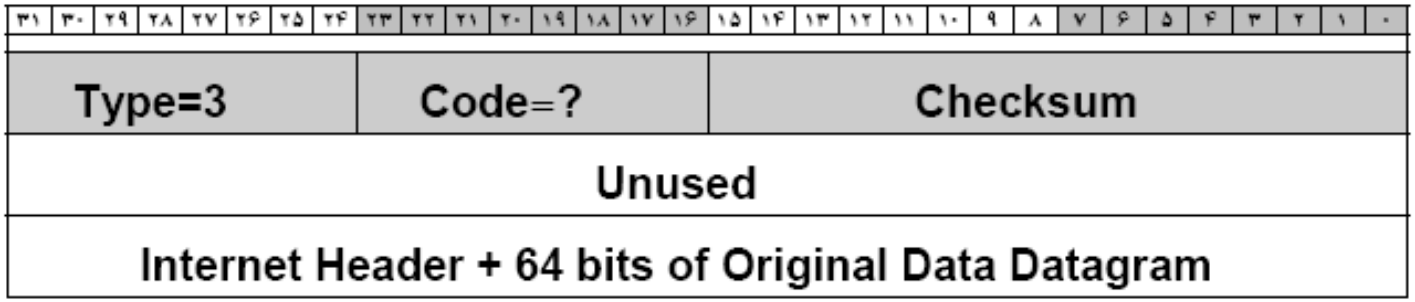
پروتکل ICMP (پروتکل پیام کنترل اینترنت) ...

انواع پیغامها در ICMP

Message type	Description	TYPE
Destination unreachable	Packet could not be delivered	3
Time exceeded	Time to live field hit 0	11
Parameter problem	Invalid header field	12
Source quench	Choke packet	4
Redirect	Teach a router about geography	5
Echo request	Ask a machine if it is alive	8
Echo reply	Yes, I am alive	0
Timestamp request	Same as Echo request, but with timestamp	11
Timestamp reply	Same as Echo reply, but with timestamp	12

♦ پیام Destination Unreachable : این پیام زمانی صادر می‌شود که زیر شبکه یا یک مسیریاب نتواند آدرس مقصد را تشخیص بدهد یا به هر دلیلی بسته توسط ماشین میزبان تحویل گرفته نشود . (مثلاً بدلیل بزرگ بودن اندازهٔ بسته‌ها و عدم اجازه به مسیریاب برای شکستن آن)

ساختار بستهٔ حامل این پیام به صورت زیر است:



معنای شماره‌های مختلف در فیلد Code به شرح زیر است:

0 : شبکهٔ مورد نظر در دسترس نمی‌باشد.

1 : ماشین میزبان مورد نظر در دسترس نمی‌باشد.

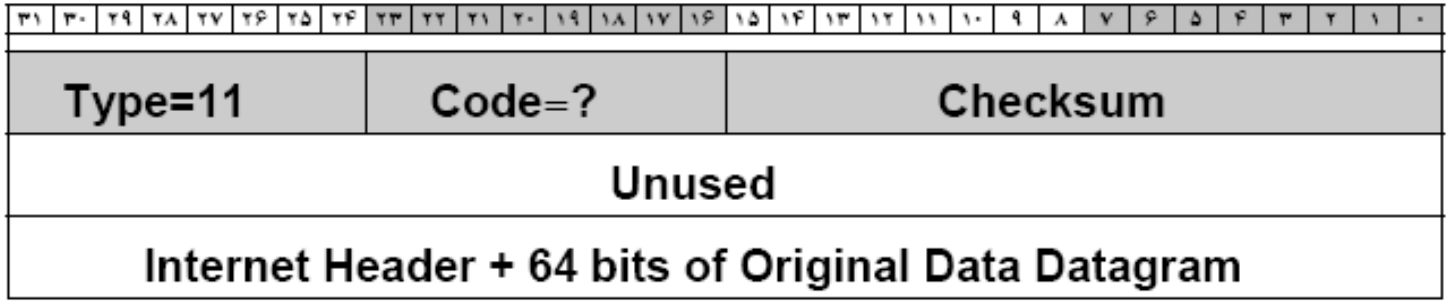
2 : پروتکل مورد نظر تعریف نشده است.

3 : شمارهٔ پورت مورد نظر وجود ندارد.

4 : اندازهٔ بسته بزرگ است و نیاز به شکستن دارد در حالی که اجازه داده نشده است.

♦ پیام Time Exceeded : این پیام زمانی صادر می‌شود که مهلت قانونی یک بسته منقضی شده باشد و یک مسیریاب مجبور شود آنرا حذف کند؛ در چنین حالتی این پیام بـه آدرس فرسـتنده بسته IP برای آگاهی ارسال خواهد شد .

ساختار بستهٔ حامل این پیام به صورت زیر است:



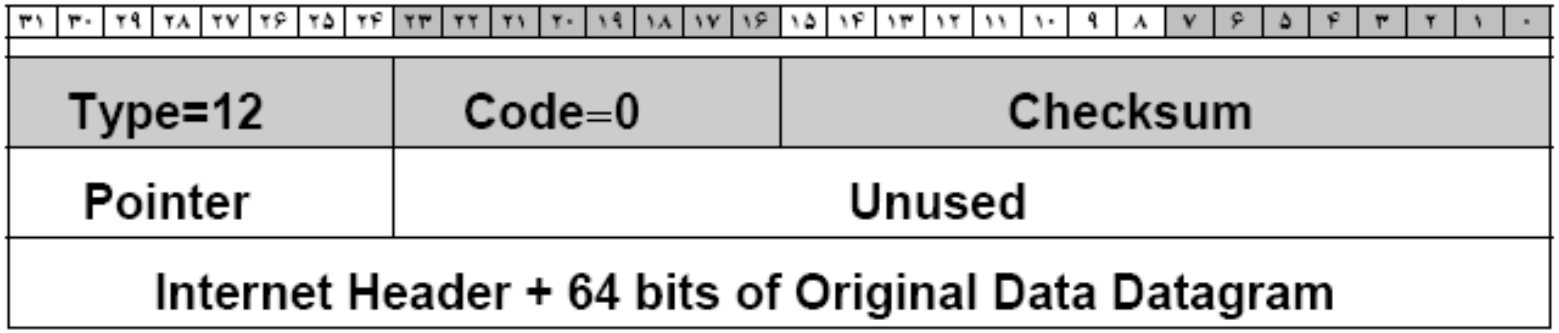
معنای شماره‌های مختلف در فیلـد Code بـه شـرح زیـر اسـت:

0 : زمان حیات بسـته منقضـی شـده اسـت. (ایـن پیـام معمـولاً توسـط مسـیریاب صـادر میشـود)

1 : زمـان بازسـازی قطعـات یـک دیتـاگـرام منقضـی شـده اسـت. (ایـــن پیـــام توســـط ماشین میزبان صـــادر میشـود)

- پیام Parameter Problem : این پیام زمانی صادر خواهد شد که مقداری نامعتبر در یکی از فیلدهای سرآیند در بسته IP قرار گرفته باشد و مسیریاب قادر به تشخیص و تفسیر سرآیند آن بسته IP نباشد. بعنوان مثال در فیلد Version از بسته IP عدد ۵ قرار گرفته باشد و یا Checksum با سرآیند تناقض داشته باشد.

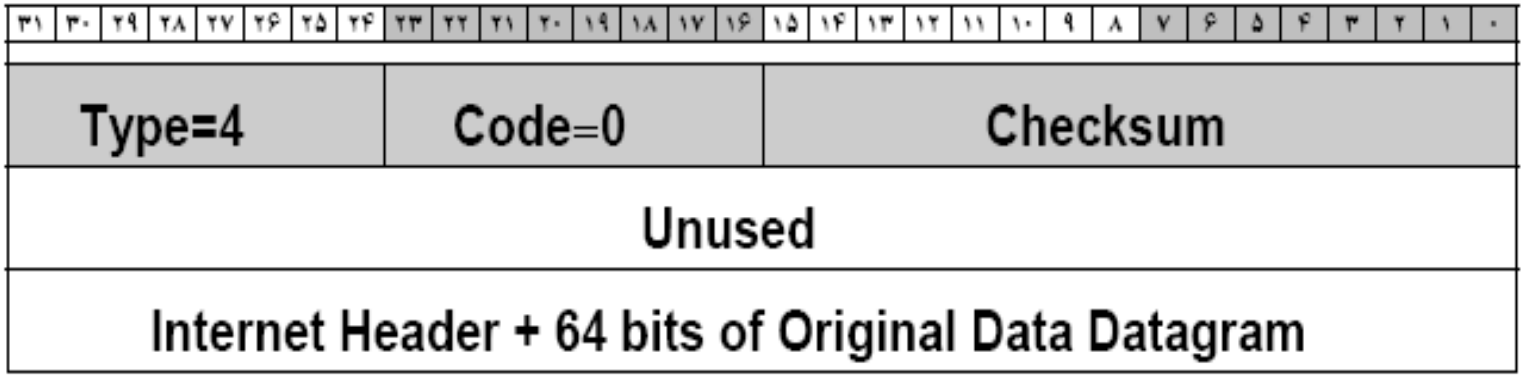
ساختار بستهٔ حامل این پیام به صورت زیر است:



فیلد Pointer محل بایتی را در بسته مشخص می‌کند که خطا در آن ناحیه بوده است.

- پیام Source Quench : این بسته زمانی برای یک ماشین میزبان ارسال می‌شود که از آن خواسته شود حجم ارسال بسته‌هایش را کاهش بدهد چرا که در غیر اینصورت ازدحام پیش خواهد آمد . در مجموع هر گاه ازیک ماشین میزبان تقاضای کاهش نرخ تولید و ارسال بسته‌های IP را داشته باشد این پیام را صادر می‌نماید. اگر ماشین میزبان پس از طی مدّت مشخصی این پیام را دریافت نکرد می‌تواند سرعت تولید بسته‌ها را به حالت اول برگرداند.

ساختار بستهٔ حامل این پیام به صورت زیر است:



- پیام Redirect : این پیـــام زمـانی صـادر می‌شـود کـه یـک مسـیریاب احـساس کنـد بسـته یا بســته‌هایی کـه بـرای او ارسـال شـده اسـت در مسـیر صحیـح نیسـتند و احتمـالاً اشـکالی در مسیریابی وجود دارد . این پیـام می‌توانـد بـرای هشـدار خطاهـای احتمـالی موثـر باشـد.

ساختار بستهٔ حامل این پیام به صورت زیر است:

۳۱	۳۰	۲۹	۲۸	۲۷	۲۶	۲۵	۲۴	۲۳	۲۲	۲۱	۲۰	۱۹	۱۸	۱۷	۱۶	۱۵	۱۴	۱۳	۱۲	۱۱	۱۰	۹	۸	۷	۶	۵	۴	۳	۲	۱	۰
Type=5								Code=?								Checksum															
Gateway Internet Address																															
Internet Header + 64 bits of Original Data Datagram																															

معنای شماره‌های مختلف در فیلد Code به شرح زیر است:

0 : باید تغییر مسیر به شبکه ای که آدرس آن مشخص شده است انجام شود.

1 : باید تغییر مسیر به ماشینی که آدرس آن مشخص شده است انجام شود.

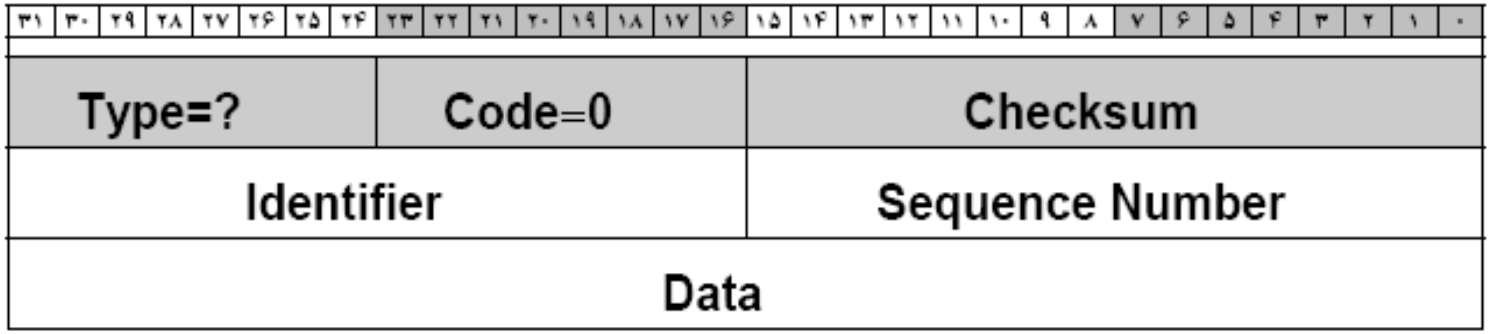
2 : برای برآورده شدن سرویس ویژهٔ درخواستی که در فیلد Type of service مشخص شده ، باید تغییر مسیر به شبکه ای که آدرس آن مشخص شده است انجام شود.

3 : برای برآورده شدن سرویس ویژهٔ درخواستی که در فیلد Type of service مشخص شده ، باید تغییر مسیر به ماشینی که آدرس آن مشخص شده است انجام شود.

فرض کنید به مسیریاب R1 بسته ای ارسال شده و او با بررسی جدول مسیریابی آنرا به مسیریاب R2 فرستاده تا او آنرا به مقصد X برساند .حال اگر R2 با مقایسهٔ الگوی زیرشبکه به این نتیجه رسید که خود او و فرستنده آن بسته در یک شبکه واقعند با ارسال این پیام به فرستنده اعلام میکند اگر از این به بعد بسته‌هایش به جای اینکه به R1 ارسال شود به R2 داده شود ، زودتر به مقصد خواهد رسید؛ ضمناً آدرس IP خودش را نیز در فیلد Gateway Internet Address قرار می‌دهد .

♦ پیغاهای Echo Request , Echo Reply : پیام Echo Request وقتی صادر می‌شود که یک مسیریاب بخواهد بداند آیا یک ماشین خاصّ شبکه قابل دسترس و موجود است یا خیر. در پاسخ به دریافت Echo Request ، مقصد با ارسال پیام Echo Reply به آن پاسخ می‌دهد . با این پرسش و پاسخ ، یک ماشین می‌تواند از قابل دسترس بودن یک مسیریاب یا ماشین میزبان در شبکه مطلع شود.

ساختار بستهٔ حامل این پیامها به صورت زیر است:



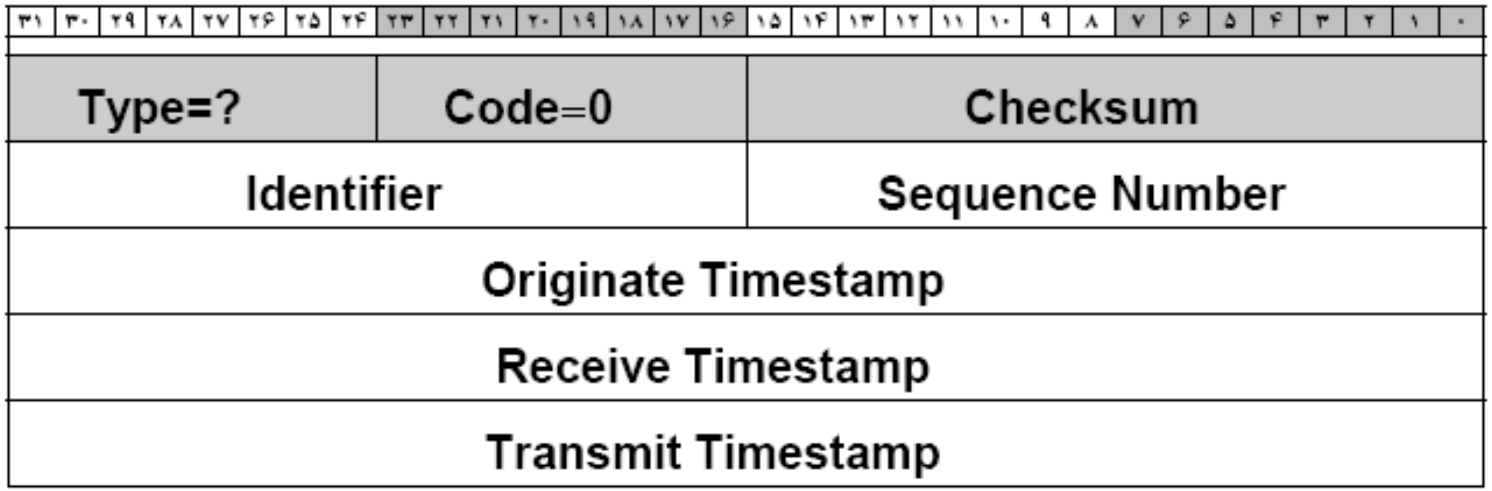
معنای شماره‌های مختلف در فیلد Type به شرح زیر است:

8 : برای مشخص کردن پیام Echo Request

0 : برای مشخص کردن پیام Echo Reply

- پیامهای Timestamp Reply و Timestamp Request : این دو پیام دقیقاً شبیه دو پیام تعریف شده در قبل هستند با این تفاوت که دریافت کنندهٔ آن ، زمان دریافت و زمان ارسال بسته را نیز در پاسخ به آن اضافه خواهد کرد. بنابراین ارسال کننده پیام Timestamp Request پس از دریافت پاسخ نه تنها از قابل دسترس بودن مقصد باخبر می‌شود بلکه زمان رفت و برگشت یک بسته را نیز می‌تواند تخمین بزند و به کمک آن جداول مسیریابی و همچنین کارائی شبکه را اندازه گیری نماید.

ساختار بستهٔ حامل این پیامها به صورت زیر است:

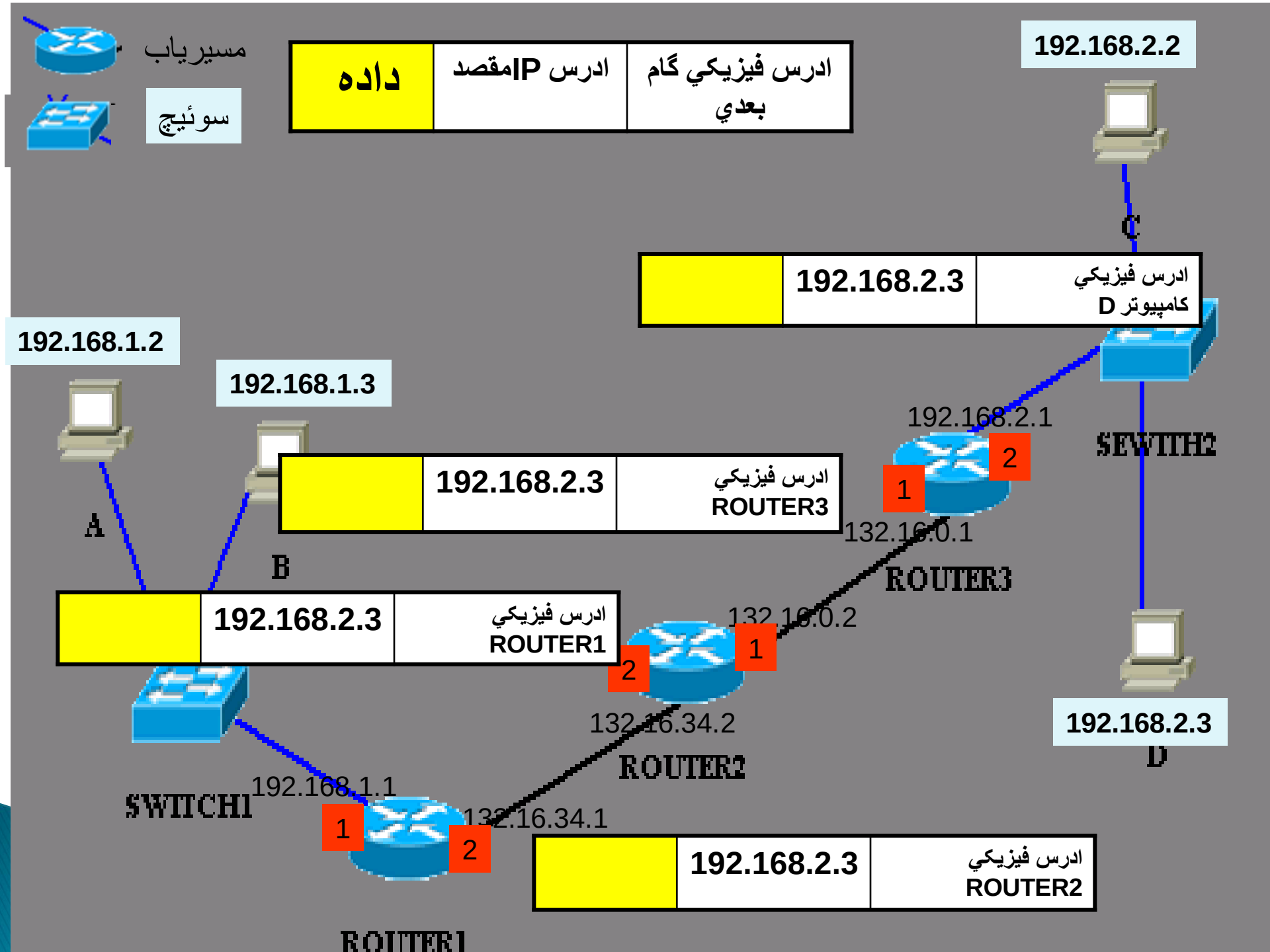


معنای شماره‌های مختلف در فیلـد Type بـه شـرح زیـر اسـت:

13 : برای مشخص کردن پیام Timestamp Request

14 : برای مشخص کردن پیام Timestamp Reply

Identifier & Sequence Number همـانند پیامـهای قبلـی بـرای پیشـگیری از اشـتباه در همخوانی و تطابق پیامهای رفت و برگشتی است. Originate Timestamp زمانی است که مبدأ ، آن پیام را ارسال کرده است (زمان بر حسب میلی ثانیه گذشته از نیمه شب و بر اسـاس زمـان جهانی گرینویچ است) . Receive Timestamp زمانی است که گیرنده آن را دریافت کرده اسـت و Transmit Timestamp زمان ارسال پاسخ بسته از طرف مقابل است . اگر زمان بر حسب میلی ثانیه آماده نبود بیت پرارزش از فیلد زمان یک می‌شود تا معلوم شود که آن فیلد معتبر نیست.


مسيرياب
سوئيچ
داده
ادرس IPمقصد
ادرس فيزيكي گام بعدي
192.168.2.2
C
ادرس فيزيكي كامپيوتر D
192.168.2.3
192.168.1.2
192.168.1.3
A
B
192.168.2.1
2
1
SEWITH2
ادرس فيزيكي ROUTER3
192.168.2.3
132.16.0.1
ROUTER3
ادرس فيزيكي ROUTER1
192.168.2.3
132.16.0.2
2
1
132.16.34.2
ROUTER2
192.168.2.3
D
SWITCH1
192.168.1.1
1
2
132.16.34.1
ادرس فيزيكي ROUTER2
192.168.2.3
ROUTER1

قسمتي ازجدول مسيريابي ROUTER2

شبکه	واسط خروجي	هزينه(تعداد گام)	
192.168.1.0	2	1	
192.168.2.0	1	1	

قسمتي از جدول مسيريابي ROUTER3

شبکه	واسط خروجي	هزينه(تعداد گام)	
192.168.2.0	2	0	
192.168.1.0	1	2	
132.16.34.0	1	1	

قسمتي از جدول مسيريابي ROUTER1

شبکه	واسط خروجي	هزينه(تعداد گام)	
192.168.2.0	1	2	
132.16.0.0	1	1	

IPV6

شاید NAT و راه حلهای دیگر تا چند سالی مشکل کمبود آدرسهای IP را حل کنند ولی مسلما نفسهای پروتکل IP به شماره افتاده است .

راه حل: IETF پروتکل IPV6 را با اهداف زیر تصویب کرد:

I. پشتیبانی از میلیارها ماشین میزبان
II. کاهش اندازه جداو مسیریابی
III. ساده سازی پروتکل بمنظور افزایش سرعت پردازش مسیریابها
IV. ارائه امنیتی بهتر از آنچه IPV4 ارائه میدهد
V. توجه بیشتر به کیفیت سرویس
VI. کمک به فرایند ارسالهای مالتی کست
VII. امکان جابجایی HOST ها بدون تغییر أدرس
VIII. امکان همزیستی با پروتکلهای جدید و قدیم
IX. امکان توسعه در آینده

ویژگیهای IPV6

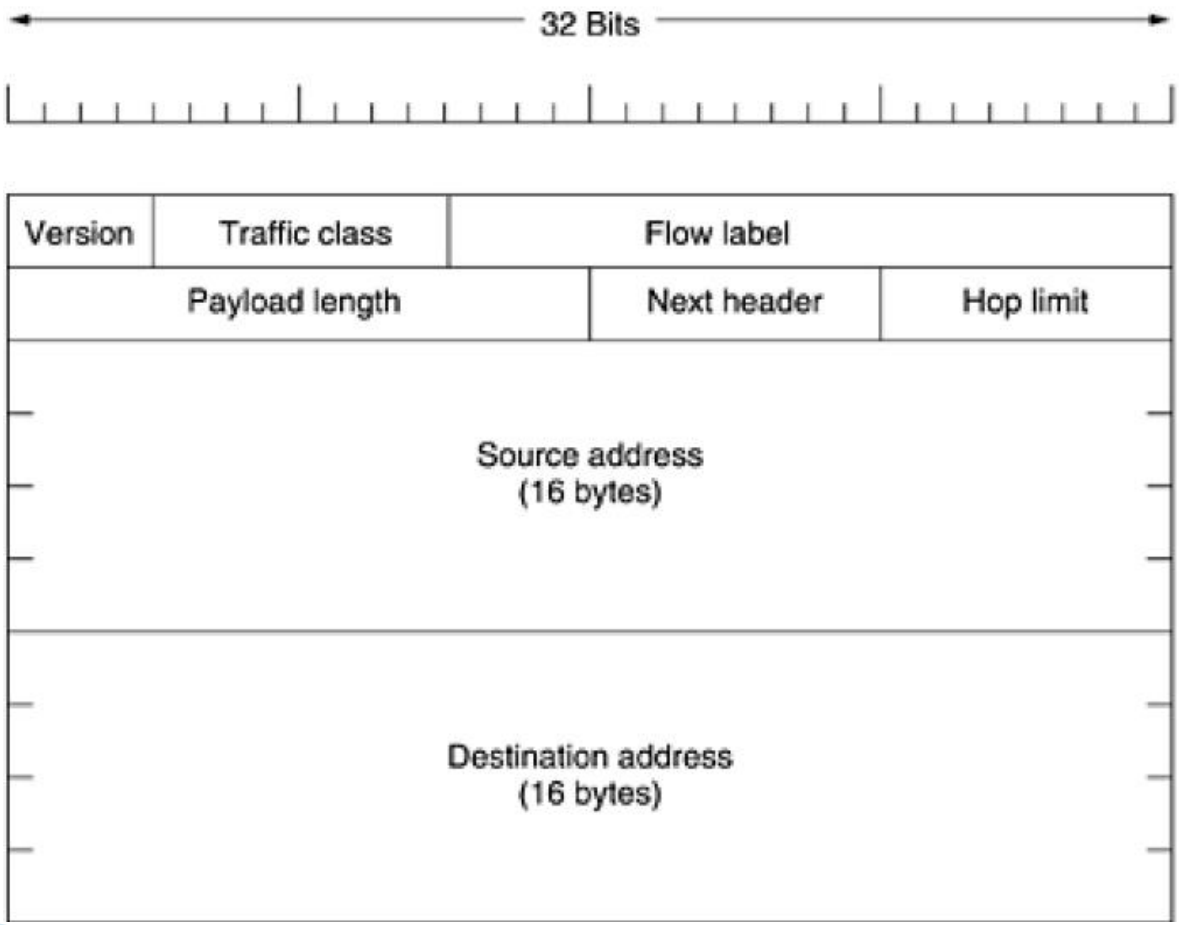
- طول آدرسها ۱۲۸ بیت است در مقابل ۳۲ بیت در آدرسهای IPV4
- سرآیند کوتاهتر(۷ فیلد در مقابل ۱۳ فیلد در IPV4)

- پشتیبانی از گزینه های اختیاری

- امنیت بالاتر(البته اگر IPSEC را جزو IPV4 در نظر نگیریم)

- توجه بیشتر به کیفیت سرویس

سرآیند ثابت والزامي IPV6



فیلدهاي سرآیند IPV6

- Version: مثل ipv4
- Traffic class: مثل type of service برای تشخیص تفاوت بسته ها از لحاظ نیازمندیهای کیفیت سرویس
- Flow label: فعلا آزمایشی است
- Payload length: سایز داده اصلی بر حسب بایت
- Next header: اگر سرآیند اضافی داشته باشیم(بجز سرآیند ۴۰ بایتی اصلی و پس از آن) این فیلد نوع سرآیند را مشخص میکند(۶ نوع سرآیند اضافی داریم).
- Hop limit: همان ttl است.
- Source Address، Destination Address

آدرسهاي ipv6

- در هشت گروه ۱۶ بیتی(یعنی در هر گروه چهار رقم هگز) که با علامت : از هم جدا شده اند نشان داده میشوند.
- مثال:

8000:0000:0000:0000:0123:4567:89AB:CDEF

برای سادگی صفرهای سمت چپ نوشته نمیشوند. اگر یک یا چند گروه صفر بود از علامت :: بجای آنها استفاده میشود: مثال بالا

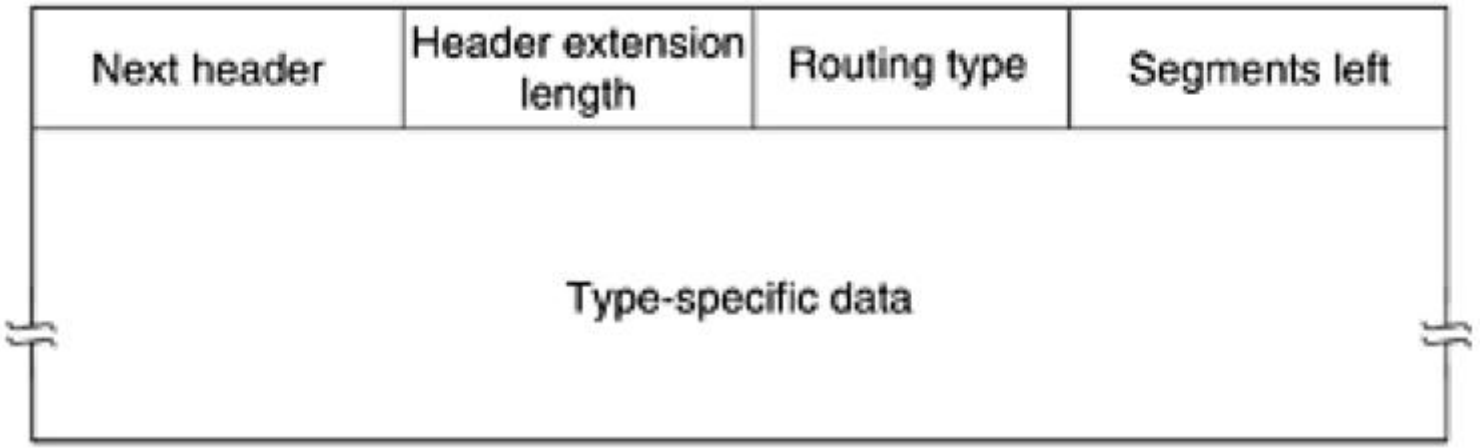
8000::123:4567:89AB:CDEF

آدرسهای IPV4 را هم بصورت زیر نمایش میدهند:

::192.31.20.46

Extension header	Description
Hop-by-hop options	Miscellaneous information for routers
Destination options	Additional information for the destination
Routing	Loose list of routers to visit
Fragmentation	Management of datagram fragments
Authentication	Verification of the sender's identity
Encrypted security payload	Information about the encrypted contents

Next header	0	194	4
Jumbo payload length			


Next header
Header extension length
Routing type
Segments left
Type-specific data

به نام خدا

طراحی و پیاده سازی زیر ساخت شبکه های کامپیوتری

مدرس: مهندس ملیحه امینی

تجهیزات شبکه

تجهیزات مورد نیاز در شبکه به 2 دسته زیر تقسیم بندی می شود:

1) تجهیزات غیر فعال شبکه

2) تجهیزات فعال شبکه

امروزه از تجهیزات تست شبکه جهت عیب یابی استفاده می گردد.

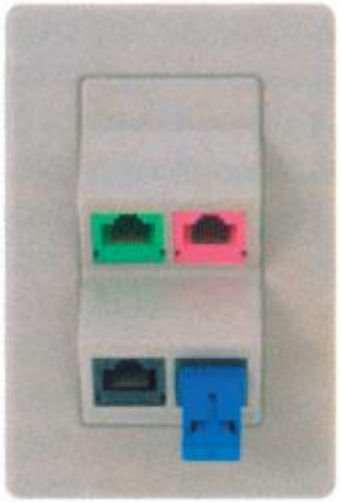
تجهیزات غیر فعال شبکه

عملکرد این تجهیزات بدون نیاز به توان الکتریکی برق صورت می گیرد.

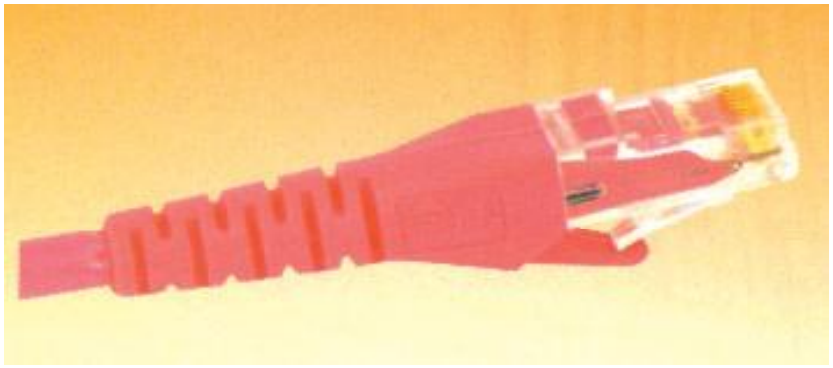
این تجهیزات عبارتند از:

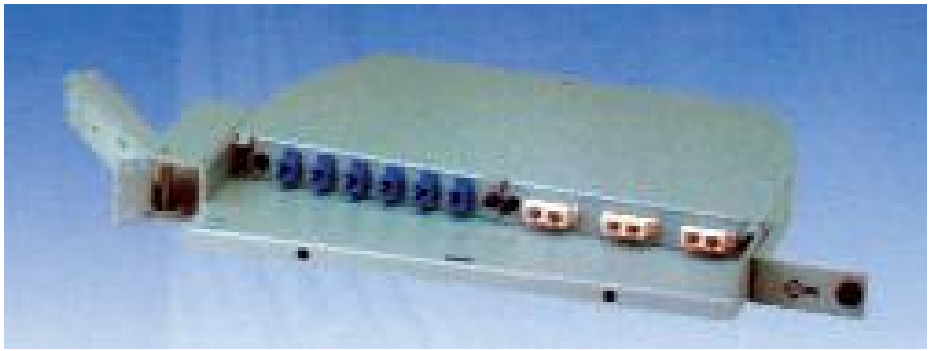
- کابلهای شبکه (کابلهای چهارزوجی و کواکسیال و فیبر نوری)
- اتصالات (کابلهای مسی و فیبر نوری و متعلقات)
- کانال و تراکینگ
- رک و متعلقات

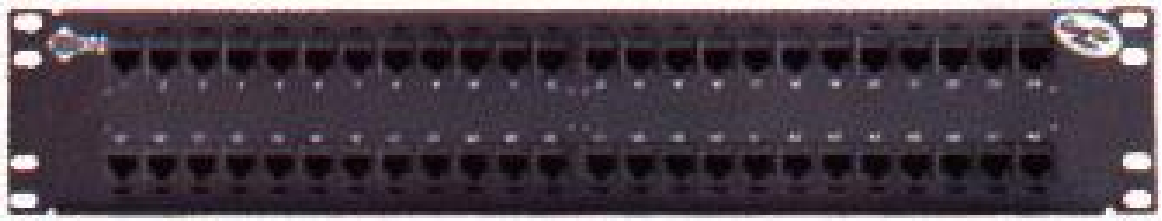
تجهیزات غیر فعال شبکه



تجهیزات غیر فعال شبکه







تجهیزات غیر فعال شبکه - کابل شبکه

- در شبکه های محلی از کابل به عنوان محیط انتقال و به منظور ارسال اطلاعات استفاده می گردد.
- نوع کابل انتخاب شده برای یک شبکه به عوامل متفاوتی نظیر :

توپولوژی شبکه، پروتکل و اندازه شبکه بستگی خواهد داشت.

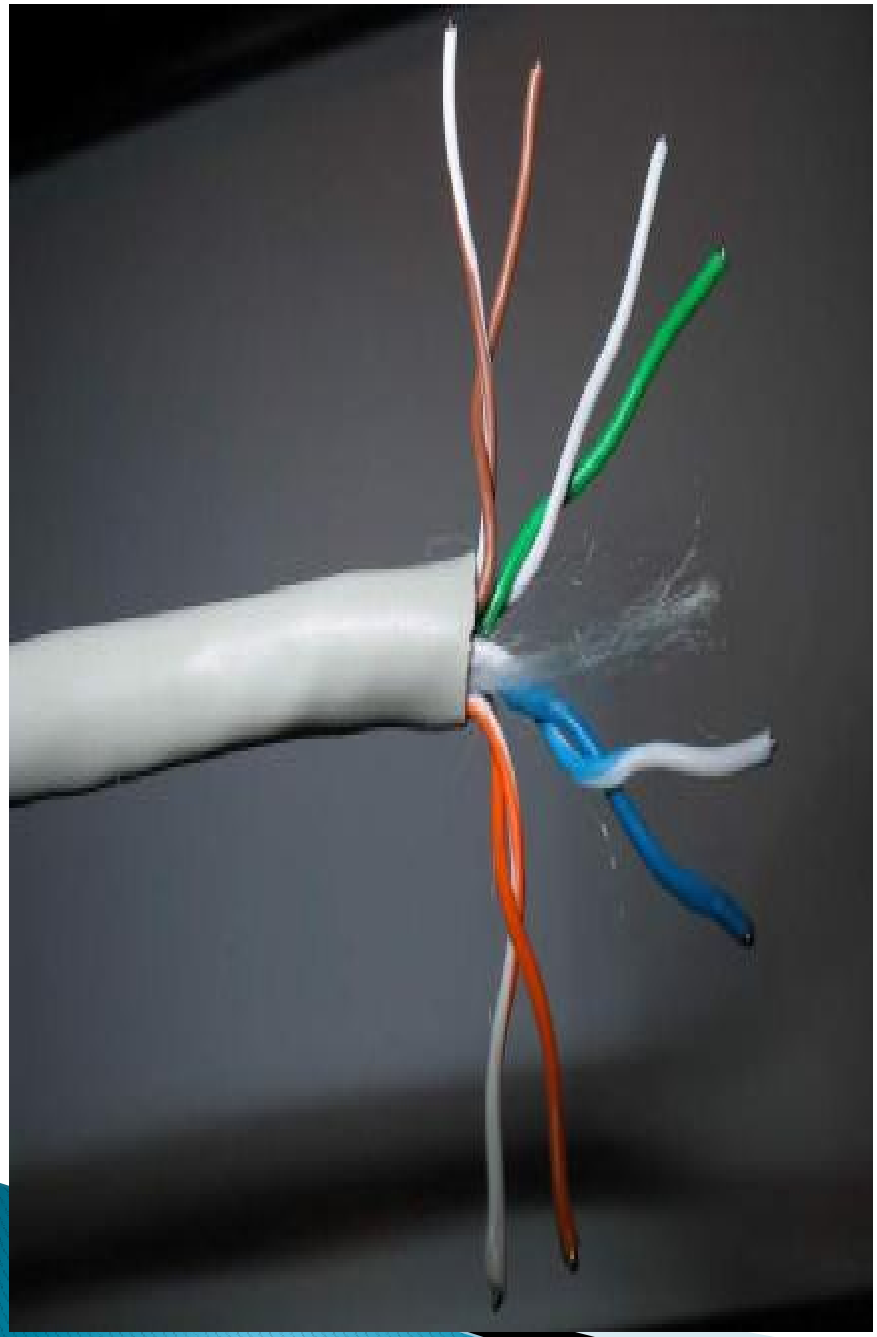
- آگاهی از خصایص و ویژگی های متفاوت هر یک از کابل ها و تاثیر هر یک از آنها بر سایر ویژگی های شبکه، به منظور طراحی و پیاده سازی یک شبکه موفق بسیار لازم است .

کابل مسی TP(Twisted Pair)

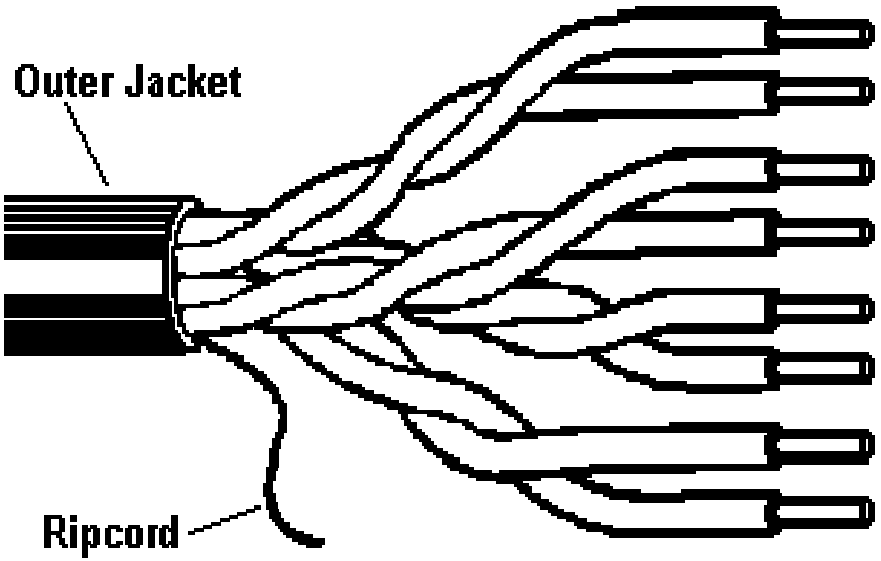
متداولترین نوع کابلی که در انتقال اطلاعات استفاده می گردد ، کابل های بهم تابیده می باشند. این نوع کابل ها دارای دو رشته سیم به هم پیچیده هستند و دارای دو دسته زیر می باشند..

UTP: نوع بدون حفاظ جفت سیم به هم تابیده شده

STP: نوع حفاظت دار این زوج سیم به هم تابیده شده



UTP Cable (4-pair)



STP

کابل مسی TP

UTP:

- بدون حفاظ
- ارزان , انعطاف پذیر , دارای قابلیت نصب آسان
- متداول ترین کانکتورهاي RJ45, UTP است

STP:

- یک میله فلزی به همراه یک پوشش پلاستیک در اطراف زوج سیم به هم تابیده شده است
- نویز پذیری کم
- گران تر بودن نسبت به UTP

انواع کابل UTP

گروه	سرعت انتقال اطلاعات	موارد استفاده
CAT1	حداکثر تا یک مگابیت در ثانیه	سیستم های قدیمی تلفن ، ISDN و مودم
CAT2	حداکثر تا چهار مگابیت در ثانیه	شبکه های Token Ring
CAT3	حداکثر تا ده مگابیت در ثانیه	شبکه های Token ring و ۱۰BASE-T
CAT4	حداکثر تا شانزده مگابیت در ثانیه	شبکه های Token Ring
CAT5	حداکثر تا یکصد مگابیت در ثانیه	اترنت (ده مگابیت در ثانیه) ، اترنت سریع (یکصد مگابیت در ثانیه) و شبکه های Token Ring (شانزده مگابیت در ثانیه)
CAT5e	حداکثر تا یکهزار مگابیت در ثانیه	شبکه های Gigabit Ethernet
CAT6	حداکثر تا یکهزار مگابیت در ثانیه	شبکه های Gigabit Ethernet

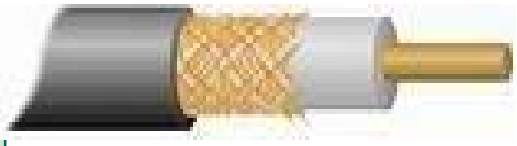
مزایای کابل های به هم تابیده

- سادگی و نصب آسان
- انعطاف پذیری مناسب
- دارای وزن کم بوده و براحتی بهم تابیده می گردند

معایب کابل های به هم تابیده

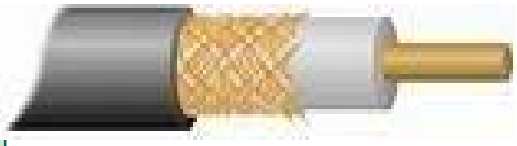
- تضعیف فرکانس
- بدون استفاده از تکرارکننده ها ، قادر به حمل سیگنال در مسافت های طولانی نمی باشند.
- پایین بودن پهنای باند
- به دلیل پذیرش پارازیت در محیط های الکتریکی سنگین به خدمت گرفته نمی شوند.

کابل کواکسیال(هم محور)



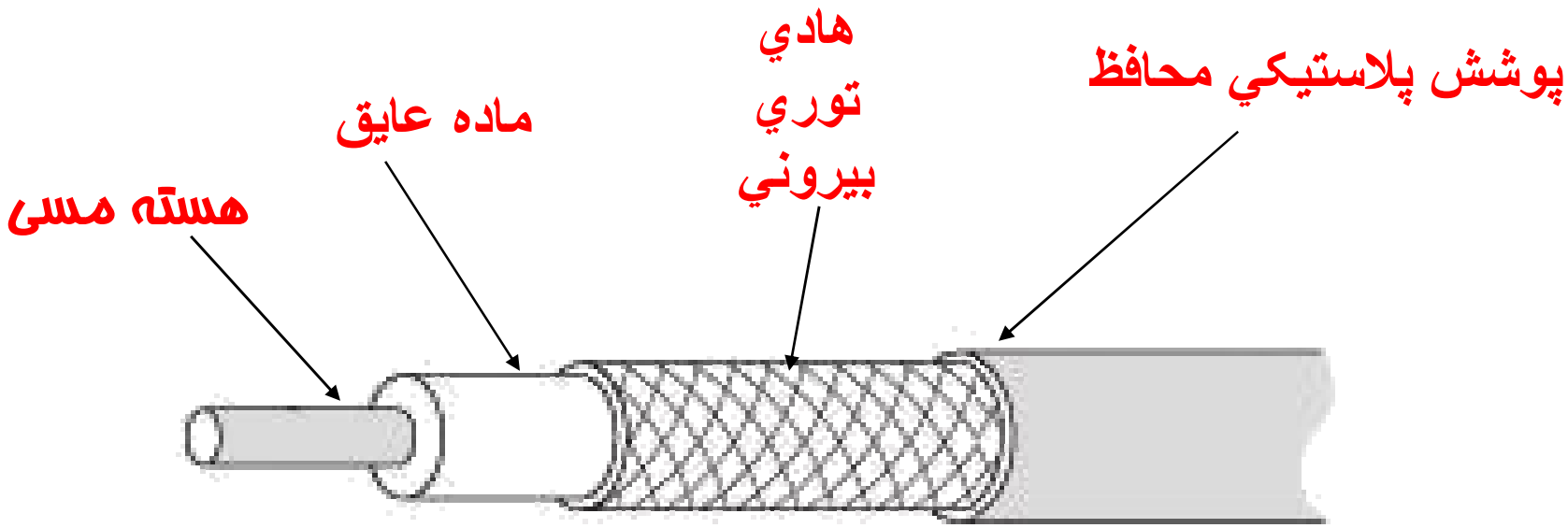
یکی از مهمترین محیط های انتقال در مخابرات کابل کواکسیال و یا هم محور می باشد . این نوع کابل ها از سال 1936 برای انتقال اخبار و اطلاعات در دنیار به کار گرفته شده اند.

کابل کواکسیال(هم محور)



این کابل متشکل از یک سیم مسی راست به عنوان هسته است که معمولاً شکننده است و توسط ماده ای عایق محاصره شده است ، عایق توسط رسانای استوانه ای پوشانده می شود که به صورت شبکه توری بافته شده است و رسانای خارجی با یک لایه محافظ پلاستیکی پوشانده شده است

کابل کواکسیال



کابل کواکسیال

کابل هم محور:

- با افزایش طول کابل سرعت انتقال داده ها افزایش می یابد
- پهنای باند زیاد(در محدوده فرکانس 100 تا 500)
- 5نوع متداول از کابل هم محور
  - G-8
  - RG-9
  - RG-11
  - RG-58
  - RG-75

مزایای کابل کواکسیال

- قابلیت اعتماد بالا
- ظرفیت بالای انتقال ، حداکثر پهنای باند 300 مگاهرتز
- دوام و پایداری خوب
- پایین بودن مخارج نگهداری
- قابل استفاده در سیستم های آنالوگ و دیجیتال
- هزینه پائین در زمان توسعه
- پهنای باند نسبتاً وسیع که مورد استفاده اکثر سرویس های مخابراتی از جمله تله کنفرانس صوتی و تصویری است .

معایب کابل کواکسیال

- مخارج بالای نصب
- نصب مشکل تر نسبت به کابل های بهم تابیده
- محدودیت فاصله
- نیاز به استفاده از عناصر خاص برای انشعابات

فیبر نوری

با گسترش شبکه ها و نیاز به پهنای باند بیشتر و مسافت طولانی تر در ابعاد شبکه ، کابل های فیبر نوری بوجود آمدند که می توانند پهنای باند بسیار بالایی را از خود انتقال دهند و تا فواصل بسیار زیاد حتی تا 2 کیلومتر از کارایی مناسب برخوردار باشند.

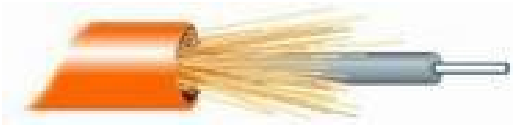
فیبر نوری

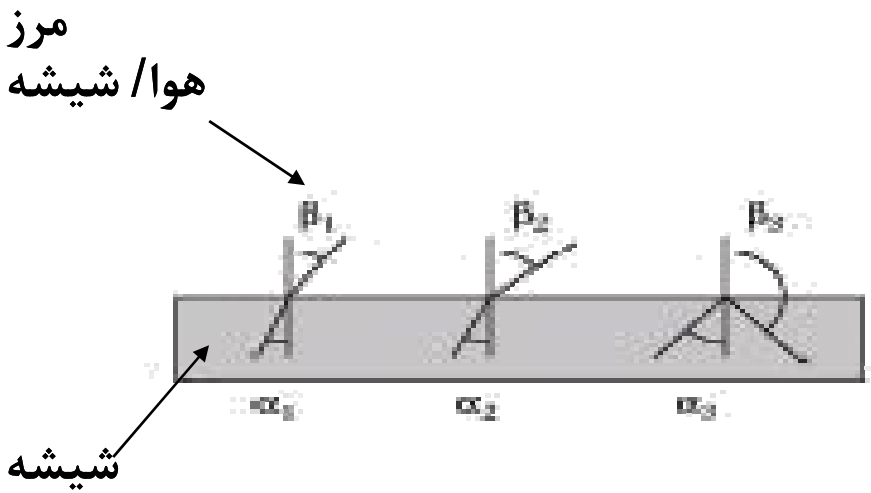
رشته هایی از شیشه یا پلاستیک که به جای انتقال سیگنال های الکتریکی ، پرتوهای نور را عبور می دهد. فناوری فیبر نوری تحولی را در سرعت ارسال داده ها و گسترش شبکه ها در فواصل طولانی بوجود آورده است .

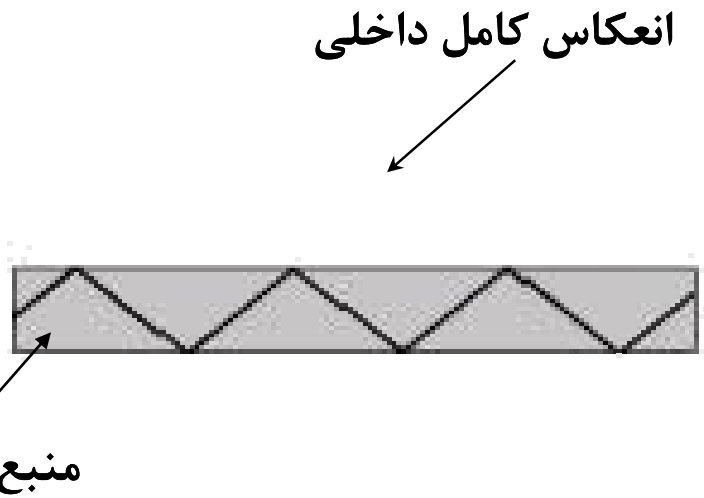
فیبر نوری

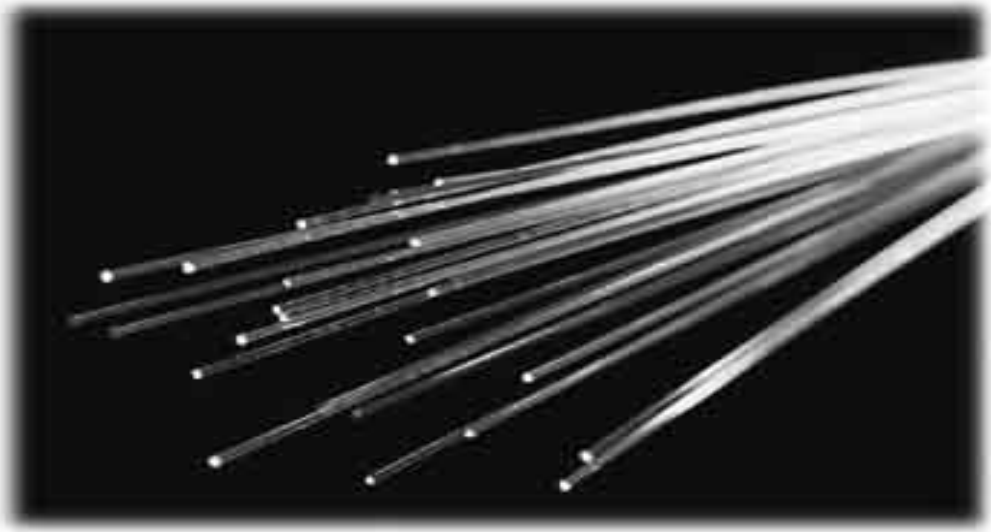
منبع نور, نور را با زاویه اي بیشتر از زاویه حد به سطح دو محیط می تاباند در نتیجه نور به داخل محیط اول بازتابش کلی پیدا می کند . این بازتابش ها بطور کلی ادامه می یابد و حتی از انحنای فیبر نوري هم پیروی می کند

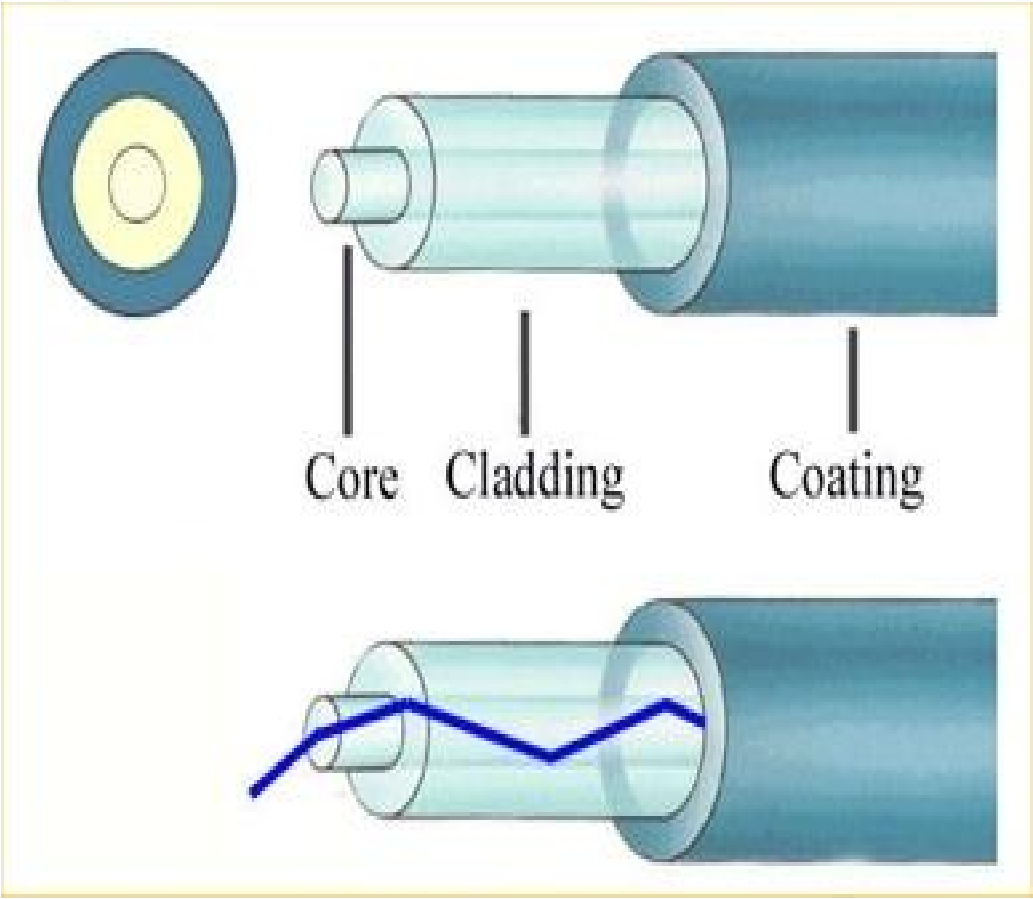
فیبر نوری










Core
Cladding
Coating

مزایای فیبر نوری

- حجم و وزن کم
- پهنای باند بالا
- تلفات سیگنال کم و در نتیجه فاصله تقویت کننده ها زیاد می گردد.
- فراوانی مواد تشکیل دهنده آنها
- مصون بودن از اثرات القاهای الکترو مغناطیسی مدارات دیگر
- آتش زا نبودن آنها بدلیل عدم وجود پالس الکتریکی در آنها
- مصون بودن در مقابل عوامل جوی و رطوبت
- سهولت در امر کابل کشی و نصب
- استفاده در شبکه های مخابراتی آنالوگ و دیجیتال
- مصونیت در مقابل پارازیت

معایب فیبر نوری

- به راحتی شکسته شده و می بایست دارای یک پوشش مناسب باشند.
- اتصال دو بخش از فیبر یا اتصال یک منبع نور به فیبر ، فرآیند دشواری است .
- تقویت سیگنال نوری یکی از مشکلات اساسی در زمینه فیبر نوری است .
- بعلت گران بودن تکنولوژی فیبر نوری و تجهیزات آن، امروزه از این فناوری در مقیاس کوچک کمتر استفاده می شود.

انواع کانکتور فیبر نوری

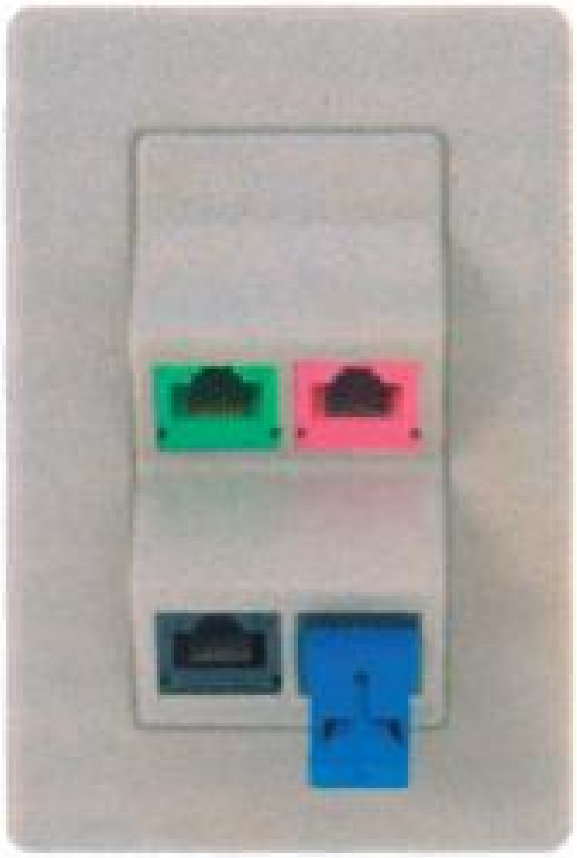
قطعه ای برای ارتباط فیبر نوری با سایر ادوات که در انواع ST، SC یا MTRJ موجود می باشد.

سر کابل مسی

قطعه ای برای ارتباط کابل مسی

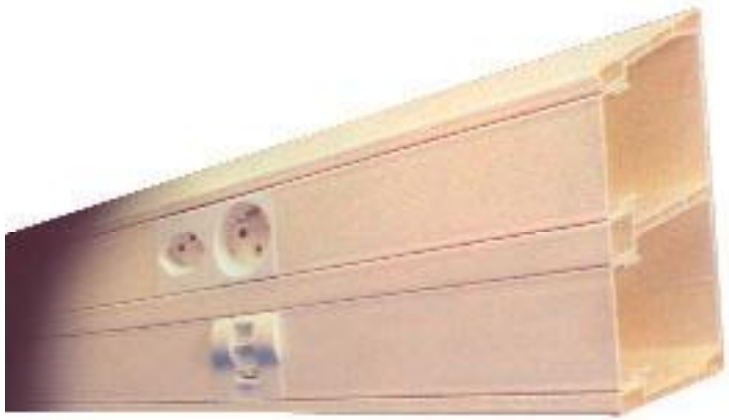
با سایر ادوات

پریز دیواری مسی



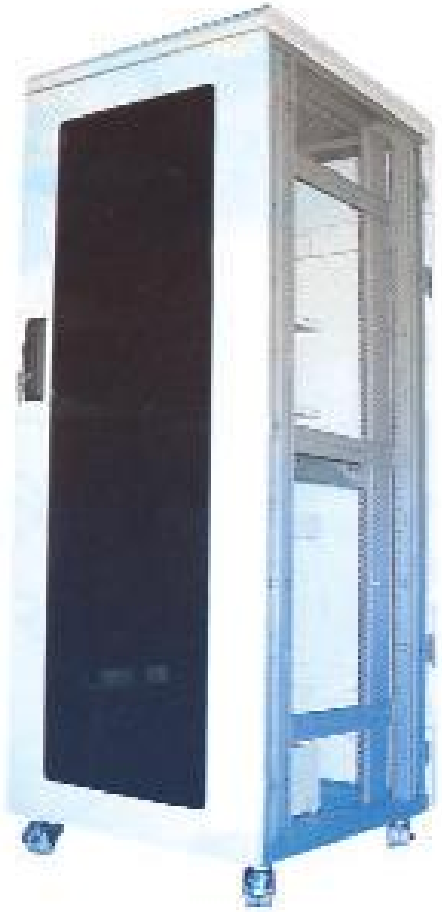
هر ایستگاه شبکه برای برقراری ارتباط با شبکه باید با استفاده از پریز اتصال فیزیکی خود را برقرار کند.

داکت یا کانال دیواری



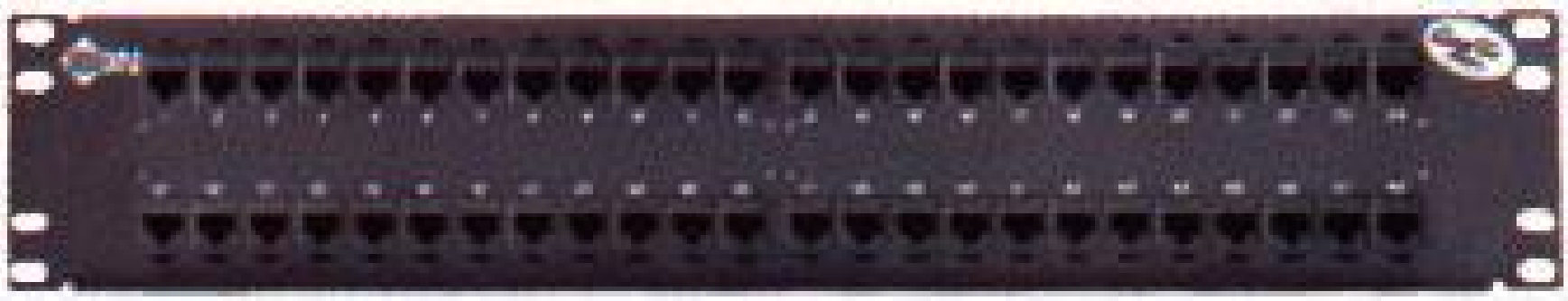
مسیری برای عبور کابل شبکه که در
انواع پلاستیکی یا فلزی و در
اندازه های مختلف ساخته می شود .

رک (Rack)



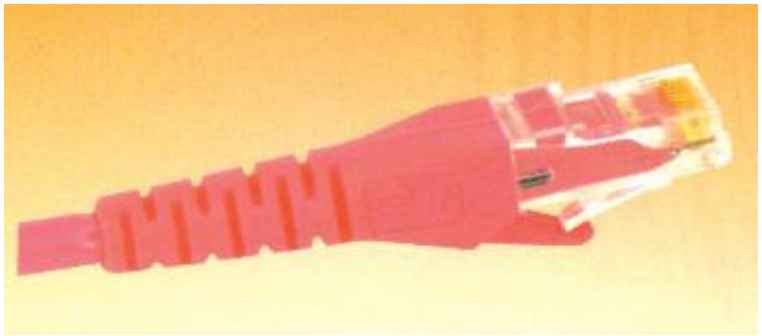
محفظه ای فلزی که محل قرارگیری سوئیچ ها , روترها , UPSیا سرور ها یا هر یک از ادوات شبکه می تواند باشد. معمولا رک ها از چهار طرف باز می شوند و شامل درب شیشه ای قفل شونده و چرخ و هواکش می باشند.

Patch panelکابل مسی



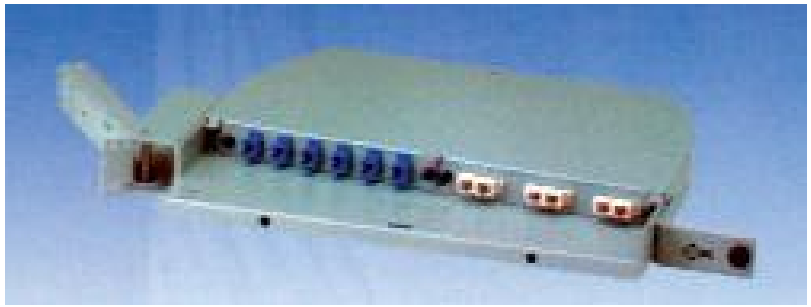
محل برقراری ارتباط بین تجهیزات اکتیو و رشته کابلهای سمت کاربران در داخل رک .

Patch cordمسی



در کابل کشی ساخت یافته برای ایجاد اتصال بین ایستگاه کاری و پریز شبکه یا اتصال تجهیزات فعال به Patch panel داخل رک از این کابل ها استفاده می شود.

Patch panelفیبر نوری



محل برقراری ارتباط بین کابل های فیبر نوری و تجهیزات فعال در داخل رک.

Patch cordفیبر نوری

در کابل کشی ساخت یافته برای ایجاد اتصال بین تجهیزات فعال با Patch panelداخل رک از قطعات کابلی به این شکل استفاده می شود.

به نام خدا

طراحی و پیاده سازی زیر ساخت شبکه های کامپیوتری

مدرس: مهندس ملیحه امینی

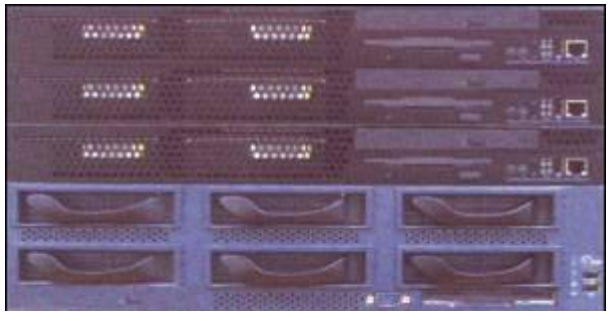
تجهیزات فعال شبکه

تجهیزاتی هستند که به جریان الکتریکی برق نیاز دارند. این تجهیزات عبارتند از:

- کارت شبکه (NIC)
- سوییچ (switch)
- مسیریاب (Router)
- دیوار آتش (Firewall)
- مبدل فیبر نوری (Media Convertor)
- صاعقه گیر
- سرور تیغه ای
- سرور
- Access Point(AP)
- آنتن

تجهیزات فعال شبکه

تجهیزات فعال شبکه



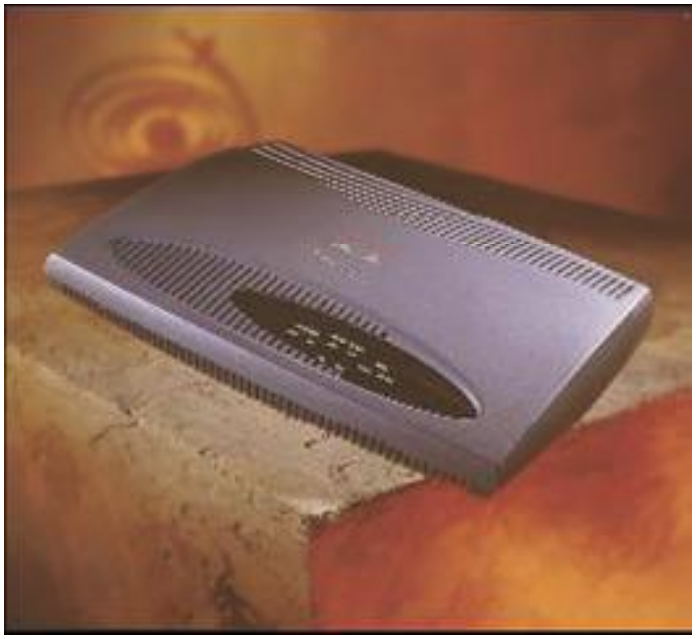
تجهیزات فعال شبکه

تجهیزات فعال شبکه - سوییچ

سوییچ ها همان قلب تپنده شبکه های starیا ستاره ای هستند که وظیفه انتقال ترافیک را بر عهده دارند .

سوییچ ها در انواع قابل نصب در رک یا غیر قابل نصب در رک و قابل مدیریت کردن یا غیر قابل مدیریت تقسیم بندی می شوند .

روتر(مسیر یاب)



مسیر یاب ها به عنوان ادواتی که در لایه ۳ شبکه کار می کنند ، وظیفه ایجاد ارتباط بین شبکه های مختلف را برعهده دارند .

مبدل فیبر نوری (Media Converter)

ابزاری برای تبدیل رسانه های مختلف به یکدیگر ، مثلا وقتی یک طرف ارتباط با کابل مسی و طرف دیگر از فیبر نوری استفاده می کند ، یکی از این تجهیزات می تواند در میان راه قرار گیرد و ارتباط دو رسانه مختلف را برقرار نماید .

مبدل فیبر نوری (Media Converter)

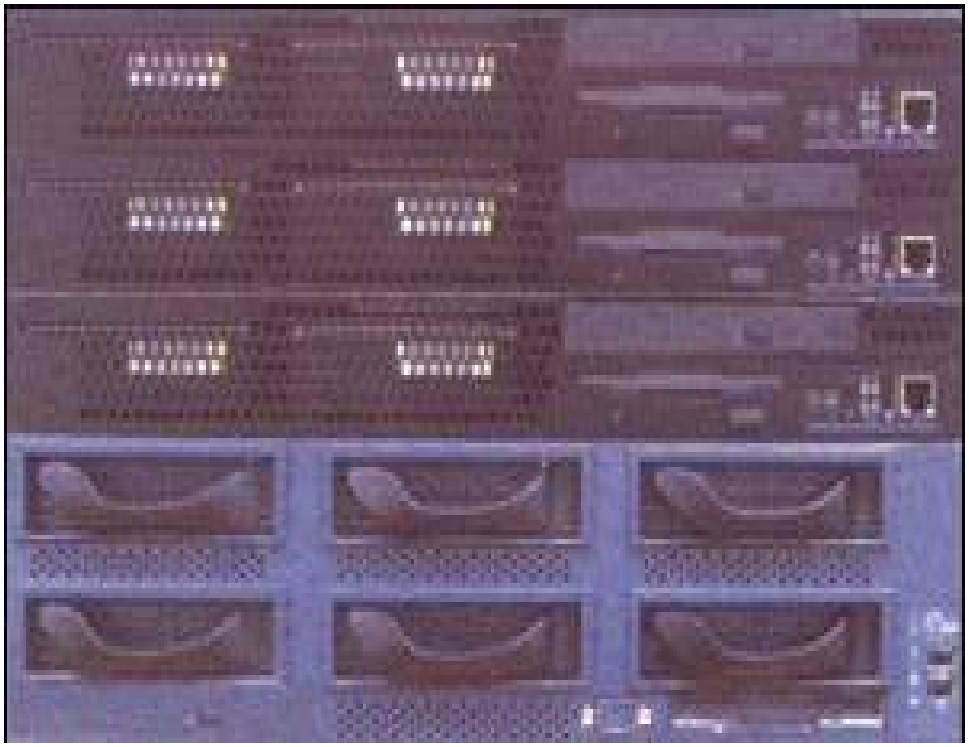
صاعقه گیر

قطعه ای در شبکه های بی سیم برای جلوگیری از آسیب های وارده به تجهیزات شبکه . به آن گاهی برق گیر نیزمی گویند .

سرور تیغه ای

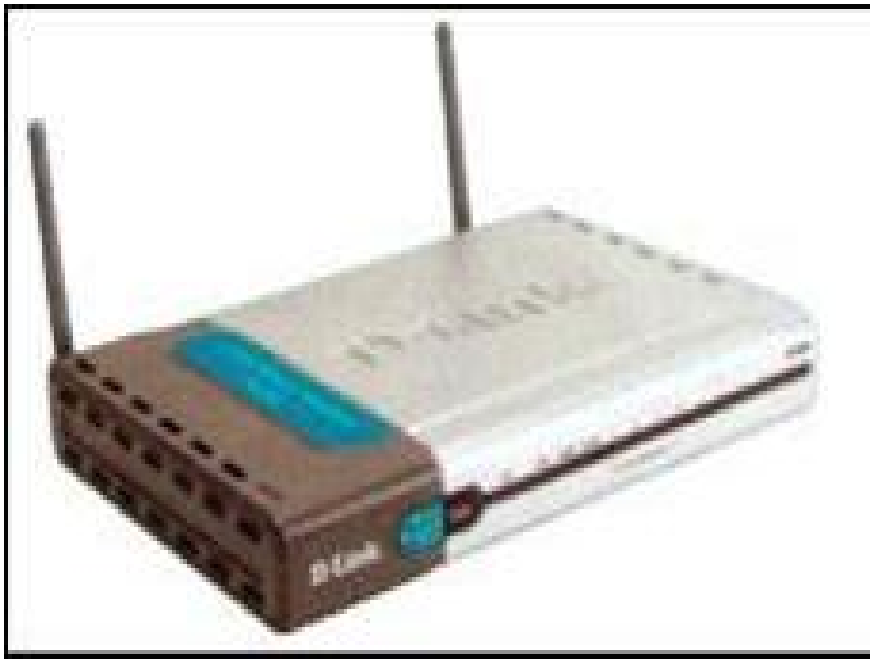
کامپیوترهای سرور را می توان در انواع تیغه های (Blade) که مناسب نصب در رک هستند تهیه نمود

سرور



سرورها در انواع مختلف ،
سرویسهای گوناگون را
به کاربران ارائه می
دهند .

Access Point(AP)



نقطه دسترسی یا APکه مشابه سوییچ و گاهی اوقات روتر در شبکه های بی سیم عمل می کند .

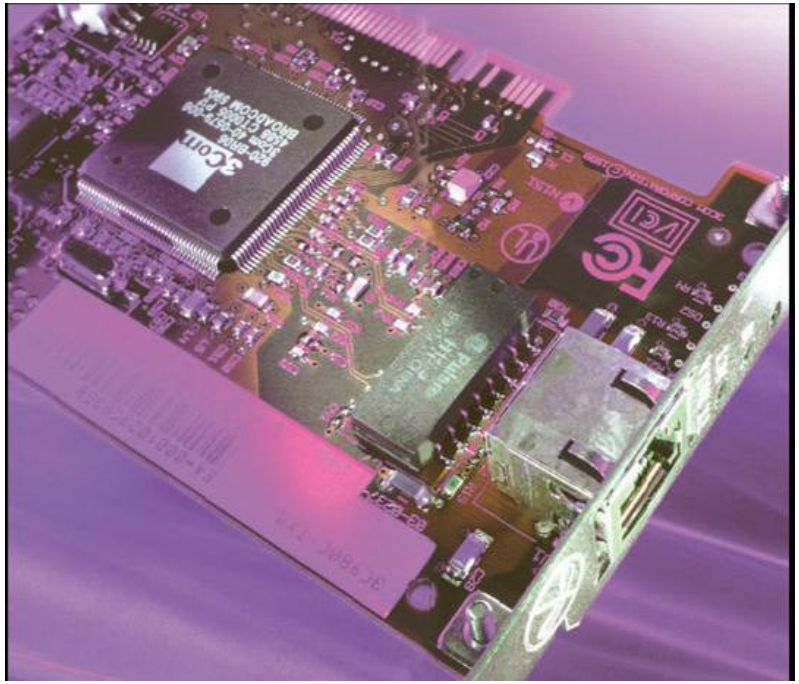
فایروال

دیواره های آتش محافظت کننده شبکه ها از حملات ویروسی ، نفوذ گران و کرم های آسیب رسان .

کارت شبکه بی سیم

نمونه کارت شبکه ای که در شبکه های بی سیم مورد استفاده قرار می گیرد .

کارت شبکه



رابط فیزیکی ایستگاه های کاری با شبکه که به NIC نیز معروف هستند .

تجهیزات شبکه بی سیم لیزری

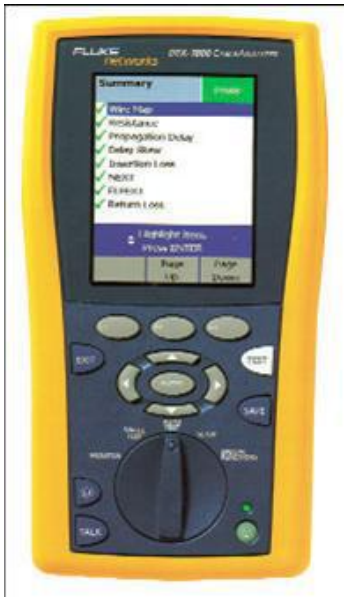
در برخی از فناوری ها ، از امواج لیزری به جای امواج رادیویی جهت ارتباط شبکه ای بی سیم استفاده می شود .

آنتن

برای دریافت امواج رادیویی درشبکه های بی سیم که به صورت Outdoor نصب می شوند به انواع متفاوتی از آنتن نیاز است .

سایر تجهیزات و متعلقات

سایر تجهیزات شبکه



سایر تجهیزات شبکه

مودم

مودمی که برای اتصال

DSL (باند پهن)

استفاده می شود.

ابزار پانچ کردن سیم کابل مسی

از این ابزار برای ارتباط کابل مسی و Patch Panel استفاده می شود .

تجهیزات ویدئو کنفرانس

ابزاری جهت برقراری ارتباط بین نقاط دوردست به صورت

ویدئو کنفرانسی

UPS

تامین کننده برق

اضطراری

مالتی پورت

مالتی پورت برای

اتصال چندین

وسیله سریال به

یکدیگر

تحلیلگر کابل

برای آگاهی از وضعیت شبکه و بستر ارتباطی ، یکی از دستگاه های بسیار خوب و کارآمد ، انواع تحلیلگرهای کابل و تحلیلگرهای شبکه می باشد .

تحلیلگر کابل

کمربند کابل

قطعه ای فلزی برای بستن و منظم کردن چندین رشته کابل

ابزار اتصال کانکتور فیبر نوری

از این ابزار برای اتصال فیبر نوری و کانکتور آن استفاده می شود .

به نام خدا

طراحی و پیاده سازی زیر ساخت شبکه های کامپیوتری

مدرس: مهندس ملیحه امینی

مراحل راه اندازی یک شبکه

مراحل راه اندازی یک شبکه

برای راه اندازی هرنوع شبکه ای مراحل زیر را باید طی کرد.

- طراحی (design)
- تنظیمات((roll out)
- پیکربندی (configuration)
- مدیریت(management)

طراحی شبکه (Design)

فاز طراحی معمولا یک الی سه روز طول میکشد که بستگی به بزرگی شبکه و کار آن دارد.

نکاتی که در فاز طراحی باید به آنها توجه کرد:

- شبکه peer-to-peerاست یا client/server
- انتخاب نرم افزار شبکه
- انتخاب زبان شبکه
- تهیه لیست سخت افزارهای موردنیاز
- تعیین میزان سطح امنیت اطلاعات
- یادگیری راه حل‌های نرم افزاری و سخت افزاری برای رفع مشکلات مدیریتی روزمره

تنظیمات شبکه (Roll Out)

برای تنظیم کردن شبکه مراحل زیر را باید انجام داد:

- آزمایش کابل‌ها
- نصب یک یا چند سِرور، اگر شبکه از نوع مدل client/server باشد.
  (برای شبکه های یکسان نیازی به کامپیوتر سِرور نمی‌باشد)
- نصب سخت افزار کامپیوترهای دیگر (گروه کاری)

تنظیمات شبکه (Roll Out) ...

- اتصال کارت‌های شبکه به کابلها (NIC-کارت شبکه باعث اتصال کامپیوترها به شبکه میشود.)
- نصب یک یا چند) hubاگر از کابل twisted pairاستفاده میشود. در این نوع شبکه ها از توپولوژی starاستفاده میشود.)
- نصب چاپگرها
- نصب برنامه سرویس دهنده (سیستم عامل شبکه یا (NOSاگر مدل شبکه client/serverاست
- نصب برنامه روی کامپیوترهای دیگر
- نصب برنامه های کاربردی

پیکربندی شبکه (Configuration)

پیکربندی شبکه به معنای سفارشی کردن آن برای کاربر است.

- ایجاد اکانت‌های دسترسی به شبکه برای کاربران (نام کاربری- کلمه عبور- گروه کاری)
- تخصیص فضایی از هارددیسک برای به اشتراک گذاشتن فایلها و داده های کاربران
- تخصیص فضایی از هارددیسک برای به اشتراک گذاشتن برنامه ها توسط کاربران (بجز برنامه های که هر کاربر میتواند از کامپیوتر خودش اجرا کند)
- تنظیم نوبت چاپ (نرم افزاری که اجازه میدهد کاربران از چاپگرهای شبکه استفاده کنند)
- نصب سیستم پشتیبانی شبکه برروی استیشن های کاربران (از این طریق کاربران میتوانند با مدیر شبکه ارتباط مستقیم داشته باشند)

اداره شبکه (Management)

- نقشه برداری از شبکه به منظور مدیریت و اشکال زدایی آسانتر
- نصب سطوح امنیتی مناسب به منظور جلوگیری از خسارات عمدی و سهوی
- بالا بردن سرعت شبکه از طریق تنظیم Lan
- ایجاد استانداردهای شرکت برای اضافه کردن سخت افزار و نرم افزار. با این کار میتوان از بروز مشکلات در آینده جلوگیری کرد.

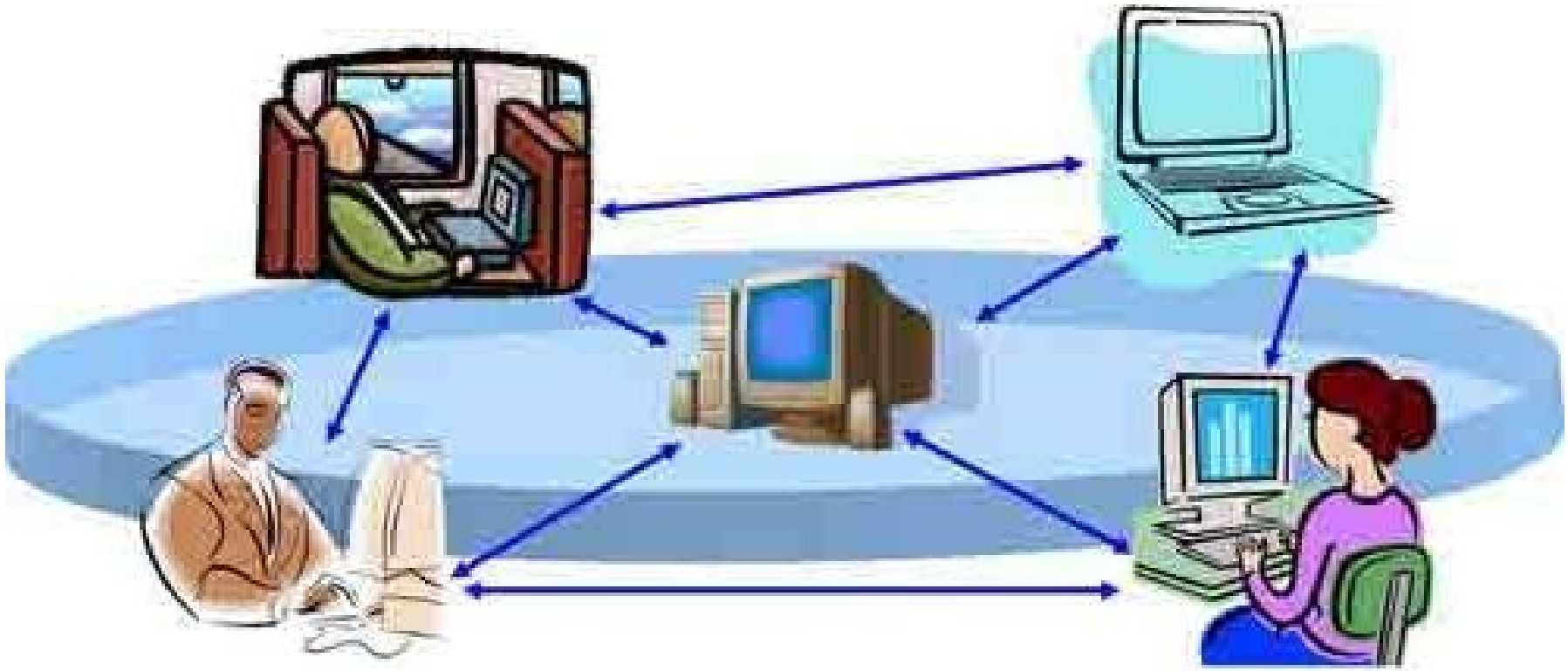
نحوه ی راه اندازی شبکه های نظیر به نظیر (Peer-to-Peer)

انواع شبکه ها از نظر ارتباطات

1. شبکه های نظیر به نظیر (Peer-to-Peer) یا یک گروه کاری
2. شبکه های بر اساس سرویس دهنده(Client - Server)
3. شبکه های مختلط (Hybrid)، که ترکیبی از نوع اول و دوم شبکه ها است.

نکته

به این نکته توجه کنید که تفاوت این دسته بندی ، با دسته بندی شبکه ها با توپولوژی های Ring , Star, bus ... در این است که توپولوژی ها، نحوه ی چیدمان کامپیوترها را مشخص می کند، ولی این دسته بندی، نحوه ی ارتباط کامپیوترها با هم را تعیین می کند. به طور مثال شما برای ارتباط 10 کامپیوتر می توانید از توپولوژی star و برای ارتباط بین کامپیوترهای موجود در این شبکه، از روش Peer-to-Peer استفاده کنید.



نوع شبکه ای که پیاده می کنید به عوامل متعددی از قبیل زیر بستگی دارد :

- اندازه ی سازمان
- سطح ایمنی مورد نیاز
- نوع کار
- سطح پشتیبانی اجرایی موجود
- میزان ترافیک شبکه (به حرکت داده های ارسالی و دریافتی در شبکه ، "ترافیک شبکه" گفته می شود)
- نیازهای کاربران شبکه
- بودجه ی شبکه

در شبکه های نظیر به نظیر هیچ کامپیوتری مسئول اداره ی کل شبکه نیست. کاربرِ هر کامپیوتر تعیین می کند که چه داده هایی در کامپیوتر او برای استفاده ی سایر کامپیوترها باید به اشتراک گذاشته شود. به عبارت دیگر هر گره در شبکه، هم سرویس دهنده است و هم سرویس گیرنده. (به کامپیوترهای داخلی یک شبکه، گره یا Nodeگفته می شود.)

پس می توان نتیجه گرفت که در شبکه های بر اساس سرویس دهنده ، کامپیوتری که در شبکه به سایر گره ها سرویس ارائه می کند ، حتما باید دارای سیستم عامل سرور باشد. ولی در شبکه های نظیر به نظیر چون یک سرویس دهنده ی مرکزی وجود ندارد، لزوما نیازی نیست که یکی از سیستم عامل ها، سرور باشد.

اندازه ی شبکه های نظیر به نظیر

شبکه های نظیر به نظیر، گروه کاری نیز خوانده می شوند. اصطلاح گروه کاری در مورد گروه کوچکی از افراد به کار می رود. در شبکه های نظیر به نظیر ، معمولا کمتر از 10 کامپیوتر در شبکه وجود دارد.

هزینه شبکه نظیر به نظیر

شبکه های نظیر به نظیر نسبتا ساده هستند. چون هر کامپیوتر به صورت سرویس دهنده و سرویس گیرنده عمل می کند، نیازی به سرویس دهنده ی مرکزی پرقدرت نیست. شبکه های نظیر به نظیر نسبت به شبکه های بر اساس سرویس دهنده ارزان تر هستند.

سیستم های عامل شبکه ی نظیر به نظیر

در شبکه ی نظیر به نظیر ، سیستم عامل شبکه نیاز به سطح توانایی و ایمنی بالایی که در شبکه های براساس سرویس دهنده لازم است را ندارد. در شبکه های براساس سرویس دهنده، سرورها فقط به صورت سرویس دهنده عمل می کنند و به صورت سرویس گیرنده یا ایستگاه کاری استفاده نمی شوند.

سیستم های عامل Microsoft Windows NT Workstation , Microsoft windows for Workgroup , Microsoft Windows 95,... قابلیت هایی برای شبکه های نظیر به نظیر دارند و نیازی به نرم افزار دیگری نیست.

شبکه ی نظیر به نظیر در کجا مناسب است؟

شبکه ی نظیر به نظیر انتخاب های خوبی برای محیط های ذیل است :

- معمولا کمتر از 10 کامپیوتر وجود داشته باشد.
- کلیه ی کاربران در فضای عمومی یکسانی (از نظر دسترسی به اطلاعات) قرار داشته باشند.
- ایمنی در درجه ی اول اهمیت مطرح نباشد.
- با توجه به موارد فوق ، گاهی اوقات شبکه ی نظیر به نظیر راه حل بهتری نسبت به شبکه ی بر اساس سرویس دهنده است.
- شبکه های نظیر به نظیر با نیازهای سازمان های کوچک سروکار دارد ، بنابر این در محیط های خاص مناسب نیست.

به طور کلی طراح شبکه، قبل از پیاده سازی شبکه موظف است به نکات زیر توجه نماید:

- مدیریت
- منابع مشترک
- نیازهای سرویس دهنده
- ایمنی
- آموزش

1 - مدیریت

مدیریت شبکه شامل امور زیر است:

- مدیریت کاربران و ایمنی
- ایجاد منابع قابل دسترس
- نگه داری برنامه های کاربردی و داده ها
- نصب و ارتقاء نرم افزارهای کاربردی

در شبکه های نظیر به نظیر، معمولا مدیر سیستم وجود ندارد که به کل شبکه نظارت کند و هر کاربر، کامپیوتر خود را اداره می کند.

2 - منابع مشترک

تمام کاربران می توانند کلیه ی منابع خود را با هر روشی که می خواهند به اشتراک بگذارند. این منابع عبارتند از فایل ها و پوشه های مشترک، چاپگرها و ...

3- نیازهای سرویس دهنده

در محیط های نظیر به نظیر هر کامپیوتر باید :

درصد زیادی از منابع خود را برای پشتیبانی از کاربر محلی (کاربرِ همان کامپیوتر) استفاده کند.

از منابع اضافی برای پشتیبانی از کاربر راه دور (کاربری که به سرویس دهنده از راه دور دسترسی دارد) برای دسترسی به منابع خویش استفاده نماید.

4- ایمنی

ایمنی شامل تعریف کلمه ی عبور برای منبعی از قبیل پوشه است که در شبکه به صورت مشترک استفاده می شود. چون تمام کاربران شبکه ی نظیر به نظیر، ایمنی مربوط به خود را تعیین می کنند و اشتراک ها می توانند به جای آنکه فقط روی سرویس دهنده مرکزی باشد، بر روی هر کامپیوتر شبکه وجود داشته باشد، کنترل مرکزی کار بسیار دشواری است. این موضوع ضربه ی بزرگی به ایمنی شبکه می زند، زیرا برخی از کاربران ممکن است هیچ گونه ایمنی را پیاده سازی نکنند. پس لازم است به این نکته توجه کنید که اگر امنیت در اولویت اول شبکه ی شما قرار دارد، از شبکه های براساس سرویس دهنده استفاده کنید.

5- آموزش

در محیط شبکه ی نظیر به نظیر، هر کامپیوتر می تواند هم به صورت سرویس دهنده و هم سرویس گیرنده عمل کند. بنابر این کاربران قبل از آنکه قادر باشند به طور مناسبی هم به صورت کاربر و هم به صورت مدیر کامپیوتر خود عمل نمایند ، باید آموزش ببینند.